PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing: 08 April 1999 (08.04.99)	
International application No.: PCT/IB98/01500	Applicant's or agent's file reference: P 1130
International filing date: 28 September 1998 (28.09.98)	Priority date: 26 September 1997 (26.09.97)
Applicant: HERRIGEL, Alexander et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

22 January 1999 (22.01.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was
[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland** Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38

82

17

PATENT COOPERATION TREATY

RECD 28 DEC 1999

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P 1130	**FOR FURTHER ACTION** See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB98/01500	International filing date *(day/month/year)* 28/09/1998	Priority date *(day/month/year)* 26/09/1997
International Patent Classification (IPC) or national classification and IPC H04N1/32		
Applicant DIGITAL COPYRIGHT TECHNOLOGIES AG et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 11 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 7 sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report
   II ☐ Priority
   III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   IV ☒ Lack of unity of invention
   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   VI ☐ Certain documents cited
   VII ☒ Certain defects in the international application
   VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
22/01/1999	22.12.99
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Moorhouse, D Telephone No. +49 89 2399 8631

Form PCT/IPEA/409 (cover sheet) (January 1994)

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-8,10-51	as originally filed			
9	as received on	28/08/1999	with letter of	26/08/1999

Claims, No.:

1-22	as received on	28/08/1999	with letter of	26/08/1999

Drawings, sheets:

1/9-9/9	as originally filed

2. The amendments have resulted in the cancellation of:

   - ☐ the description, pages:
   - ☒ the claims, Nos.: 23-42
   - ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

   - ☐ restricted the claims.
   - ☐ paid additional fees.
   - ☐ paid additional fees under protest.

☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

   ☐ complied with.

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

   ☒ all parts.

   ☐ the parts relating to claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-22
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-17
	No:	Claims	18-22
Industrial applicability (IA)	Yes:	Claims	1-22
	No:	Claims	

2. Citations and explanations

   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Concerning Box IV

The following document is cited :-

D1 : Delaigle et al.: "Digital Watermarking", Proceedings of the SPIE, Vol. 2659, February 1996, pages 99-110

Comparison of the first alleged invention (claims 1 to 17) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- encoding a watermark using at least one key of an asymmetric cryptographic key pair,
- encrypting the stego data set using the key pair, and
- transmitting the encrypted stego data set.

Comparison of the second alleged invention (claim 18) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- generating at least one message
- digitally signing said message using an asymmetric cryptographic key pair, and
- using the signature as a seed for watermark generation.

Comparison of the third alleged invention (claims 19 and 20) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- calculating at least some magnitude Fourier components of a cover data set,
- applying an authentification function to said components to generate an authentification message,
- encrypting the authentification message using a secret key of an asymmetric cryptographic key pair, and
- embedding said encrypted message as a payload in a public watermark.

Comparison of the fourth alleged invention (claims 21 and 22) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:

- transmitting a hash value of the stego data set to a registration party, and
- storing certification data at the registration party, the certification data comprising a hash value of the stego data set, a digital time stamp and information designating the originator of the stego data set.

Thus, the differences between the claims of the different groups of inventions and the disclosure of document D1 are totally different between invention groups. Therefore, the independent claims on file are not linked together by a **single general inventive concept**, as required by Rule 13.1 PCT.

The IPEA chose not to invite the Applicant to pay additional examination fees pursuant to Rule 68.1 PCT since, as pointed out above, the lack of unity seemed to arise (for the most part) from the choice of claim wording adopted and the desire to protect subpart of the invention, and could have been remedied by appropriate wording amendments.

Concerning Box V

The following further documents were cited in the Written Opinion :

D2 : EP-A-0 534 419

D3 : Zhao et al: "Embedding Robust Labels into Images for Copyright Protection", Proceedings of the Knowright Conference, Proceedings of The International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technology, 21st August 1995, pages 242-251, XP000603945

D4 : Ruanaidh et al: "Phase Watermarking of Digital Images", Proceedings of The International Conference on Image Processing (IC, Lausanne, Sept. 16th - 19th, 1996, Vol. 3, 16th September 1996, pages 239-242, XP000199952, Institute of Electrical and Electronics Engineers

D5 : FR-A-2 740 897

D6 : EP-A-0 539 726

The following documents are cited for the first time in this Report, following the drafting of certain claims as being indisputably independent :

D7 : Delaigle J.-F. et al: 'Digital Images Protection Techniques in a Broadcast Framework: An Overview', PROCEEDINGS OF THE EUROPEAN CONFERENCE ON MULTIMEDIA APPLICATIONS, SERVICES AND TECHNIQUES, Vol. 2, 28 - 30 May 1996, pages 711-727, XP000199920, Louvain la Neuve (BE)

D8 : Zhao et al: 'A WWW Service to embed and prove digital copyright watermarks' PROCEEDINGS OF THE EUROPEAN CONFERENCE ON MULTIMEDIA APPLICATIONS, SERVICES AND TECHNIQUES, vol. 2, 28 - 30 May 1996, pages 695-709, XP000199921, Louvain la Neuve (BE)

As pointed out with respect to clarity and Box VIII below, various claims lack clarity. Nonetheless, should these clarity objections be met during further prosecution of this application in the national / regional phase, then the comments below regarding inventive step would be applicable.

Claims 1 to 17
The subject-matter of these claims requires that, rather than a single private key, an asymmetric pair of cryptographic keys is used in both generating a watermark and in encrypting the watermarked data. Whilst, as set out in the prior art summary below, both asymmetric key pairs and watermarks using such pairs are known, there is no prior art document which suggests that the same pair be used for watermarking and encrypting the watermarked data set. This would appear to be a step back from what would be the result of a combination of document D7, disclosing the use of asymmetric cryptographic key pairs, with, for example, a document D2 relating to cryptography in general, namely that, for full security, different keys should be used for watermarking and final encryption of the result of watermarking.

Claim 18
The subject-matter of this claim is rendered obvious by the disclosure of document D3, and thus does not meet the requirement set out in Article 33 (3) PCT.

Document D3 teaches the skilled person that a message, relating to features extracted from an image to be watermarked, can be digitally signed using a private key and then used as a seed for watermark generation (in particular, for seeding the positions at which said watermark is inserted) - see the top of page 244. The only difference with respect to the subject-matter of independent claim 18 is the use of an asymmetric cryptographic key pair. Despite the arguments of the Applicant relating to the complexity of such key pairs, the IPEA does not consider that this fact alone would put the skilled person off at least considering using them in place of a private key. Moreover, claim 18 does not specify how the method is adapted to the use of an asymmetric cryptographic key pair. Thus, the subject-matter of claim 18 is derivable in an obvious manner from the disclosure of document D3.

Claims 19 and 20

The subject-matter of these claims is rendered obvious by the disclosure of document D4 taken in combination with the disclosure of any of the documents D1, D3 and D7, and thus does not meet the requirement set out in Article 33 (3) PCT.

Document D4 teaches the skilled person how to generate a watermark using a Discrete Fourier Transform, by altering, inter alia, the phase components resulting from the application of said transform. It would be obvious to adapt the teaching of document D4 such that the process of independent claim 30, requiring modification of the magnitude components, is carried out, particularly since this possibility is also hinted at in the disclosure of document D4.

Moreover, each of the documents D1, D3 and D7 discloses the use of keys in watermarking. Their use to control the insertion of the watermarks disclosed in document D4 is thus an obvious measure to take. The remarks made above with respect to the use of asymmetric cryptographic key pairs are applicable to claim 19 also.

Claims 21 and 22

The subject-matter of these claims is rendered obvious by the disclosure of document D8, and thus does not meet the requirement set out in Article 33 (3) PCT.

Document D8 teaches the skilled person how to generate a stego data set and transmit it between two parties, whilst registering certification data at a third party (see the paragraph labelled (3) at the top of page 705). The only difference between this disclosure and the subject-matter of independent claim 39 is the use of a hash function

instead of a cryptographic key in the latter. However, such hash functions and their advantages are well known in the art, and their use in the context of the system disclosed in document D8 thus cannot be considered as being of any inventive significance.

Concerning Box VII

The claims are not in the two-part form defined in Rule 6.3 (b) PCT.

The inclusion by reference of the priority document may be objectionable under certain national or regional jurisdictions (e.g. Europe).

The abbreviation "IAD" appearing on page 13, line 33 has not been previously defined.

Concerning Box VIII

Claims 1, 4, 6, 7, 12, 18 and 19 lack clarity and/or support in the description, and therefore do not meet the requirement set out in Article 6 PCT.

Claim 1

This claim is far too vaguely and speculatively worded. It is, for example, not clear from the present claim, how the various levels of security referred to in the description are realised, since only one watermark and only one key need be used, according to certain claimed alternatives. In the case of the other alternatives, i.e. more than one watermark and a second (public) key, it is completely obscure what is done with these items. For example, if only one key of a pair is used ("at **least** one" means one, or more than one), is it the private or the public key. In the former case, their is very little difference with respect to certain prior approaches. In the case of two keys, are different watermarks protected differently ?

From the description it would appear that a detection watermark is embedded, followed by a first layer of cryptographic protection, followed by embedding of a private watermark, followed by more cryptographic protection, followed by embedding of a public watermark and finally a third layer of cryptographic protection (see, in particular, pages 23 and 24).

It is furthermore not clear, whether "encoding" in the claim is the same as "encrypting" in the description, as "encoding" is never actually defined in the description.

Claim 4

There is no support in the description for the features of this claim, in particular pages 30 to 33 (section IIIb) do not mention modulation of the phase components.

Claim 6

The wording "encoded" is objected to for reasons set out above with respect to claim 1. It is not clear, where in the description there is support for use of more than one watermark *of the first type*.

Claim 7

Claim 6 implies that the first watermark is the private watermark (which, according to pages 23 and 24 is the type of watermark which is encrypted using the private key (ps_H), whereas the public watermark is encrypted using the public key (vs_H)). Claim 7 then implies that the first (private) watermark is encrypted using a hash value, which contradicts said description pages.

Claim 12

It is not at all clear from the claim, what "erased elements" might be. Why, and by whom or what have they been erased ? The claim per se must define what this wording means.

Claim 18

It is not at all clear what is meant by the wording "generating at least one message", because neither the starting data nor the resulting data is defined.
By analogy with the objections to claim 1, it is not clear, what the public key of the pair is used to encrypt, and what the private key is used to encrypt.

Claim 19

It is not clear what is meant by "calculating *at least some* magnitude Fourier components".

It is not clear what an "authentification *value*" is. In line with the description, the wording "an authentification message" should have been used on this claim.

It is not clear from the "embedding" strep, that this step uses the public key.

propose a digital signature scheme for watermarking facsimile documents (binary images). This scheme modify the length of certain runs of data with a single bit of the signature data.

Disclosure of the Invention

It is an object of the present invention to provide a system of the type mentioned above that provides a simple and secure way of generating and transmitting watermarked data. This object is achieved by the methods described in the claims.

In one aspect of the invention, this object is achieved by an integrated solution method for generating and transmitting a data set between two parties H and B comprising the steps of a) providing a cover data set corresponding to the data set to be transmitted, b) generating a stego data set of said cover data set by embedding at least one digital watermark in said cover data set, wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair of H, said key pair comprising a secret private key and a known public key derived therefrom, and c) encrypting said stego data set using said key pair of H, d) transmitting said encrypted stego data set from said party H to said party B.

Preferably, the private and public keys of party H are an elliptic curve key pair.

The party creating the watermark can embed a detection, a private and a public watermark in the data set, wherein the detection or the private watermark is derived from the private key, the public watermark from the public key. The public watermark can be detected by third parties while the private watermark can only be detected using private information. Preferably, the detection or private watermark is not derived from the private key directly but from a hash value of the same and/or from a signature generated with the same, such that the

amended Sheet

PCT Chapter II
MU DG2

Einschreiben

Europäisches Patentamt

D-80298 München

Zurich, 26. August 1999
Patents Dr. SU/io
Our File: P 1130

Application No. 98947703.9- /PCT/IB9801500
Digital Copyright Technologies AG

Dear Sirs

Enclosed please find amended pages 9, 52 – 56 and one page 57 – 63 for replacing the current pages 9, 52 – 63.

The following amendments have been made:

- Claims 19 – 38 have been cancelled.
- Original claims 41 and 42 now carry the numbers 19 and 20.
- Original claims 39 and 40 now carry the numbers 21 and 22.
- In claim 4, "phase components" has been replaced by "magnitude components". This is disclosed on page 34, step 5 of the description: It is the magnitude components of the Fourier transform that are being modified with the pseudo-random vector **m** (see also page 31, line 33).
- Claim 6 has been amended for better clarity by cancelling the word "further" (that was objected to by the examiner) and by replacing "at least a first watermark" by "at least one

watermark of a first type". The "watermark of a first type" can either be the "private watermark" or the "detection watermark" described on page 23, lines 26ff and 31ff. For encoding both these watermarks, the private key ps_H has been used: for the detection watermark, the value $crh(ps_H)$ is used as a first argument in the function OWEA; for the private watermark, ps_H enters as a first argument in function $DSSMR_G$, the result of which is again used as a first argument in function OWEA.

- Claims 7 and 8 have been amended according to the changes in claim 6.
- Similar to claim 6, the expression "second watermark" of claim 9 has been amended to "watermark of a second type". Also, claim 9 has been corrected to state that the Fourier transform is calculated on the *cover* data, not the *stego* data, as correctly pointed out by the examiner.
- In claim 10, step ii, "at least one key" has been replaced by "a key".
- In claim 18, "especially for step b) of one of the preceding claims," has been deleted.
- In claims 19, 21 (original claims 41, 39), "especially of one of the preceding claims," has been deleted.
- On page 9, lines 27, 28, it has been added that the private and public keys of party H are an elliptic curve key pair. This was disclosed in original claim 5.

Claim 1

a) Inventive step of claim 1:

The problem to be solved by the present invention is to provide a simple and secure way for generating a stego data set and transmitting the same. This method is solved by claim. The stego data set is generated by embedding at least one watermark into it. The watermark is encoded using a key of an asymmetric cryptographic key pair. The stego data set is then encrypted using *the same* key pair.

In contrast to known techniques, such as those described in D1 and D2, the same keys are used for protecting the watermark as well as the transmission. This simplifies the key management on the copyright owner's side (only one pair of keys must be maintained) as well as the verification of the received message and watermark (because not only message

recovery/verification, but also watermark detection/verification can profit from the same key infrastructure).

It is not disputed that D1 teaches the skilled person to generate a watermark using, inter alia, a copyright owner's secret key. D1 does, however, not specify what kind of key this is. It simply says that the key must be secret. A normal computer user often uses a large number of such secret keys, mostly in the form of passwords. The user manages them himself and privately.

Asymmetric cryptographic key pairs, as described in D2, are well known for encrypting messages. They consist of a private and a public key. The public key is usually registered at a trusted party. Also, asymmetric cryptographic key pairs are usually fairly long in order to provide good security, hence the private key is usually not a simple password but a passphrase or a long series of digits.

Because of their length, because of the fact that they come in pairs, because of the need for their registration and because of their narrow scope of application, asymmetric cryptographic key pairs are therefore usually not regarded as "just another secret key" that can be used for any suitable purpose. Hence, a person skilled in the art would not think it obvious to "abuse" them wherever a secret key is required. In particular, just because D1 suggests to use a secret key for encoding a watermark, it would not be obvious to use a key of an asymmetric cryptographic key pair for this purpose.

Only *after* overcoming the prejudice against "abusing" the asymmetric key pair, a person skilled in the art would consider the consequences of using them for watermark generation. It would therefore be retrospective to assert that the above mentioned advantages would encourage the person skilled in the art to use the key pair as claimed.

As to the arguments at the top of sheet four of the communication of 01. 07. 99, it is stated that "D2 teaches the skilled person how to increase cryptographic security by using an asymmetric key pair" and that it would therefore "be obvious to apply the teaching of this document to the teaching of document D1". However, it is not clear how the *encryption mechanisms* taught by D2 could be applied to increase security in the method according to claim 1 of the present application, since claim 1 uses encryption in step c only.

Clarity of claim 1:

As explained above, the features of claim 1 have the following consequences: The same keys are used for protecting the watermark as well as the transmission. This simplifies the key management on the copyright owner's side (only one pair of keys must be maintained) as well as the verification of the received message and watermark (because not only message recovery/verification, but also watermark detection/verification can profit from the same key infrastructure).

Hence, claim 1 provides a solution to the problem mentioned above, i.e. to provide a simple way for generating a stego data set and transmitting the same, in particular by making key management and watermark verification easier.

It is true that the embodiment described by the application is much more complex, using several watermarks, etc., which provides additional advantages. However, the features listed in the claim 1 are per se sufficient to reach the above advantageous consequences. Hence, there is no need to narrow claim 1.

Decision T 1055/92 of the boards of appeal of the European patent office states in its headnotes:

1. *The form and content of the claims in a European patent application are governed by the requirements of Article 84 and Rule 29 EPC. According to Article 84, the claims shall define the matter for which protection is sought.*

   This function of the claims should be clearly distinguished from the requirement that the European patent application must disclose the invention in such a way that it enables a person skilled in the art to carry out that same invention.

2. *Under Article 83, sufficient disclosure is required in a European patent application, i.e. in the application as a whole, comprising the claims, together with the description and the drawings, but not of an individual claim as such.*

3. *A claim in a European patent application must comprise the essential features of the invention (see T 32/82, OJ EPO 1984, 354); the essential features should in particular comprise those features which distinguish the invention from the closest prior art.*

Even though this decision is based on the articles of the European Patent Convention, it is fully applicable to the corresponding regulations of the PCT.

In the present case, claim 1 does comprise all the "essential features", i.e. those features which distinguish the invention from the closest prior art.

As to the term "encoding" that was objected to, it is the same term as used in the description, see e.g. page 19, lines 25 and 35, page 20, lines 1, 4, 7 and 37, page 28, lines 33 and 35, etc. The feature "encoding the watermark using at least one key..." of claim 1 relates to the fact that the watermark is generated using this key, e.g. by using the function OWEA as described on pages 23 and 24 of the application.

It is not clear what the opinion means by the sentence "Moreover, it is not clear how the claimed subject-matter solves the problem set out in the description relating to the copyright holder having to reveal the private key, since on of the claimed alternatives reales to use only of the public key" on sheet 6, 4th paragraph.

When the copyright holder uses his private key for encoding the watermark (as it is done in phase 3 on page 23 of the application), he simplifies the watermarking process because he does not need to keep track of additional secret keys. When he uses his public key (as is done in phase 4 on page 24 of the application), the buyer has a means for verifying if the watermark is indeed embedded in the picture by relying on the public key of the copyright holder.

Claim 4

The examiner's comments regarding claim 4 are gratefully acknowledged. The claim has been amended accordingly, see above.

Claim 5

The examiner objects that claim 5 is not supported by the description. The features of claim 5 have therefore been added to page 9, lines 27, 28 of the description.

Claims 6, 7

The objections regarding claim 6 should be overcome by the amendments mentioned above. As explained above, the term "watermark of a first type" refers to either the detection watermark or the private watermark. Claim 7, where the watermark is generated using the

hash value of the private key, refers to the detection watermark. The claim is therefore not in contradiction with the description.

Claim 9

It has been objected that in the disclosure there is no support for more than one second watermark. Claim 9 is clearer now as it says that at "least one watermark of a second type" is generated. As described on page 33, lines 36ff, the cover image can be divided into a plurality of adjacent blocks, wherein a watermark is applied to each block, hence more then on watermark can be generated.

Claim 10

The objection against claim 10 should be overcome by the above amendment.

Claim 12

It is stated that it is unclear what "erased elements" can be. The claim says that **m'** has the same length as the symbol vectors. However, depending on how **m** is embedded into the data and on what changes the data "suffers" before the watermark is read, some information may obviously be lost. For instance, if **m** is added to some Fourier components of an original image and the image is then "shrunk", some Fourier components may be lost, i.e. *erased*, in which case it would not make sense to say that **m'** has the same length as the symbol vectors. Hence, claim 12 should be clear: it just implies that, if some elements have been lost due to imperfect transmission/handling of the stego data, **m'** may of course loose some of its elements.

Claim 18

Claim 18 has been rejected as being obvious in view of D1 and D2. However, same as claim 1, it suggests using an asymmetric key pair when generating a watermark. As explained for claim 1 above, the application of asymmetric key pairs in the generation of watermarks is unusual and not obvious. We refer to our arguments relating claim 1.

Claim 19 (corresponding to original claim 41) also involves using an asymmetric key pair in watermark generation.

Claim 21 (corresponding to original claim 39) has been rejected as being obvious in view of D6. It is, however, not true that D6 teaches "how to generate a stego data set and transmit it between two parties whilst registering certification data at a third party" and that "the only difference between this disclosure and the ... claim ... is the use of a hash function instead of a cryptographic key in the latter".

D6 teaches that each party is equipped with a "configuration vector", which defines the cryptographic permissions it has. When registering its keys, a party transmits the configuartion vector to a trusted party, which then generates a key certificate. Subsequently, secure transmissions between different parties are carried out *without* involving the trusted party.

In contrast to this, the claimed method relates to a transmission between two parties H and B that does involve a trusted third party. In addition to this, claim 21 comprises the step of generating a stego data set from the cover data set, which finds no correspondence in D6.

In fact, D6 is concerned with a technical field that is very different from the claimed method. In D6, the trusted third party ensures the integrity of keys and prevents the parties from using cryptographic operations without permission. The present application relates to an improvement in the transmission of watermark protected (stego) data. Hence, a person skilled in the art would not even consider D6 when looking for a solution to the problem solved by the present application.

It is therefore believed that the present claims are allowable over the state of the art.

Further amendments to the description are put off until entry into the regional phase.

If the Examiner finds it advisable to conduct an informal telephone conference in order to expedite the examination, she/he is invited to contact the undersigned.

Very truly yours,
E. B L U M & C O.
i.V.

Dr. K. Sutter

Enclosures: – Replacement pages
– Confirmation of receipt and return envelope

propose a digital signature scheme for watermarking facsimile documents (binary images). This scheme modify the length of certain runs of data with a single bit of the signature data.

Disclosure of the Invention

It is an object of the present invention to provide a system of the type mentioned above that provides a simple and secure way of generating and transmitting watermarked data. This object is achieved by the methods described in the claims.

In one aspect of the invention, this object is achieved by an integrated solution method for generating and transmitting a data set between two parties H and B comprising the steps of a) providing a cover data set corresponding to the data set to be transmitted, b) generating a stego data set of said cover data set by embedding at least one digital watermark in said cover data set, wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair of H, said key pair comprising a secret private key and a known public key derived therefrom, and c) encrypting said stego data set using said key pair of H, d) transmitting said encrypted stego data set from said party H to said party B.

Preferably, the private and public keys of party H are an elliptic curve key pair.

The party creating the watermark can embed a detection, a private and a public watermark in the data set, wherein the detection or the private watermark is derived from the private key, the public watermark from the public key. The public watermark can be detected by third parties while the private watermark can only be detected using private information. Preferably, the detection or private watermark is not derived from the private key directly but from a hash value of the same and/or from a signature generated with the same, such that the

Claims

1. A method for generating and transmitting a data set between two parties H and B comprising the steps of

a) providing a cover data set (CD) corresponding to the data set to be transmitted,

b) generating a stego data set (SD) of said cover data set (CD) by embedding at least one digital watermark in said cover data set (CD), wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair (ps_H, vs_H) of H, said key pair comprising a secret private key (ps_H) and a known public key (vs_H) derived therefrom,

c) encrypting said stego data set (SD) using said key pair (ps_H, vs_H) of H,

d) transmitting said encrypted stego data set from said party H to said party B.

2. The method of claim 1, wherein said step c) comprises

generating a mask message (B||SN),

generating a signature ($DSSMR_G(ps_H$, B||SN)) of said mask message (B||SN) using said secret private key (ps_H), and

using said signature of said mask message for seeding an encryption algorithm for said stego data set (SD).

3. The method of claim 2 wherein said signature ($DSSMR_G(ps_H$, B||SN)) of said mask message (B||SN) is transmitted from H to B.

4. The method of one of the claims 2 or 3 wherein said encryption algorithm comprises the step of calculating the Fourier transform of said stego data set

(SD), modifying the phase components of the Fourier transform using a pseudo-random pattern seeded by said signature ($DSSMR_G(ps_H, B||SN)$) of said mask message ($B||SN$) and calculating the inverse Fourier transform for generating the encrypted stego data set.

5. The method of one of the preceding claims wherein said key pair (ps_H, vs_H) of H is an elliptic curve key pair.

6. The method of one of the preceding claims wherein said step b) comprises the step of generating at least one watermark of a first type, wherein said watermark of a first type is encoded using said private key (ps_H) of H.

7. The method of claim 6 wherein said watermark of a first type is encoded using a hash value ($crh(ps_H)$) of said private key (ps_H) and can be decoded by using said hash value ($crh(ps_H)$).

8. The method of claim 6 wherein said watermark of a first type is encoded using a hash value ($crh(OAD_{CD})$) of a signature (OAD_{CD}) generated using said private key (ps_H).

9. The method of one of the preceding claims wherein said step b) further comprises the step of generating at least one watermark of a second type, wherein said watermark of a second type comprises a payload ($pc_H[AM]$) derived from the Fourier transform of said cover data (CD).

10. The method of one of the preceding claims wherein said step b) comprises the steps of:

i) providing a message ($s_1, s_2, \ldots, s_M$) to be transmitted in said at least one watermark, said message consisting of a plurality of symbols,

ii) providing a pseudo random generator seeded with a seed value derived from a key of said key pair (ps_H, vs_H) of H or a hash value thereof,

iii) encoding said message using values from said pseudo random generator

iv) using the said encoded message (**m**) for embedding said watermark.

11. The method of claim 10 wherein said step iii) comprises:

for each of said symbols (s_i), generating a pseudo random sequence of numbers ($v_1, v_2, \ldots$) by a said pseudo random generator,

using the value of each said symbols (s_i) for selecting a sub-sequence within said pseudo random sequence for forming a symbol vector ($\mathbf{r}_i$), and

adding said symbol vectors ($\mathbf{r}_i$) to generate said encoded message (**m**).

12. The method of claim 11 comprising the following steps for decoding said message:

extracting a read-out message (**m'**) from said watermark, said read-out message being a vector having the same length, if erased elements are replaced by zero, as said symbol vectors ($\mathbf{r}_i$),

generating all possible values of said symbol vectors ($\mathbf{r}_i$) using said pseudo random generator seeded with said seed, and

calculating the cross-correlation between said pseudo random sequences of numbers ($v_1, v_2, \ldots$) and said read-out message (**m'**) for retrieving said symbols (s_i).

13. The method of claim 10 wherein said step iii) comprises:

for each bit (b_j) of said symbol sequence (s_1, s_2, ..., s_M), deriving pseudo random vectors ($\mathbf{r}_j{}^*$) having elements 1 or -1 from a said pseudo random generator, which pseudo random generator preferably generates m-sequences or Gold codes, and

depending on the value of said bit (b_j), multiplying said pseudo random vector ($\mathbf{r}_j{}^*$) with +1 or -1 to generate a modified pseudo random vector, and adding said modified pseudo random vectors to generate an encoded message (**m**).

14. The method of claim 13 comprising the following steps for decoding said message:

extracting a read-out message (**m'**) from said watermark,

deriving said pseudo random vectors ($\mathbf{r}_j{}^*$) from said pseudo random generator seeded with a said seed, and

calculating the cross correlation between each of said pseudo random vectors ($\mathbf{r}_j{}^*$) and said read-out message (**m'**) for retrieving the corresponding bit (b_j) of the said symbol sequence (s_1, s_2, ..., s_M).

15. The method of one of the claims 10 - 14 wherein the position of components to be modulated by each value of the encoded message (**m**) is given by a pseudo random generator seeded by a key known by both H and B.

16. The method of one of the preceding claims comprising the step of encoding a message for being embedded in said watermark by using symbol based Reed Solomon codes as error control codes.

17. The method of one of the preceding claims wherein said step b) further comprises the step of calculating a logarithm of said cover data set (CD) before embedding said watermark for embedding said watermark in a perceptually flat domain.

18. A method for generating a stego data set (SD) from a cover data set (CD) comprising the steps of:

generating at least one message (ID_{CD}),

digitally signing said message (ID_{CD}) using an asymmetric cryptographic key pair (p_H, v_H) and a signature generating algorithm (DSSMR) with message recovery for generating a digital signature (OAD_{CD}), and

generating said stego data set (SD) of said cover data set (CD) by generating at least one digital watermark, wherein said digital signature (OAD_{CD}) is used for deriving a seed for generating said watermark.

19. A method for embedding a watermark in a cover data set for generating a stego data set, comprising the steps of

calculating at least some magnitude Fourier components (MC) of said cover data set (CD),

applying an authentication function (AF) for generating a value (AM) derived from said Fourier components (MC),

ciphering said value (AM) using a secret key (pc_H) of an asymmetric key pair (pc_H, vc_H) for generating a ciphered message, and

embedding said ciphered message as a payload in a public watermark.

20. A method for verifying the originality of a possibly modified stego data set generated with the method of claim 19 comprising the step of reading said value (AM) by decoding said ciphered message using the

public key of said key par and comparing said magnitude Fourier components to said stego data set.

21. Method for generating and transmitting a data set between two parties H and B, comprising the steps of

providing a cover data set (CD) corresponding to the data set to be transmitted,

generating a stego data set (SD) of said cover data set (CI) at a party H by generating at least one digital watermark in said cover data set (CD),

transmitting a hash value of said stego data set (SD) to a registration party (O), and

permanently storing certification data (CCD) at said registration party (O), said certification data comprising said hash value of said stego data set (SI), a digital time stamp (TVP) and information designating said party H.

22. The method of claim 21 further comprising the steps of generating a digital signature of said certification data (CCD) using an asymmetric cryptographic key pair (ps_O, vs_O) of said registration party (O), transmitting said certification data (CCD) and said digital signature to said party H, and verifying said digital signature at said party H by using a public key (vs_O) of said key pair of said registration party.

PATENT COOPERATION TREATY

From the:
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

E. BLUM & Co.
Vorderberg 11
8044 ZÜRICH
SUISSE

5 - JULI 1999

V	N	A

LPA	NF	MR	Vw	Bh	A	K
2			1			

PCT

WRITTEN OPINION

(PCT Rule 66)

Date of mailing *(day/month/year)*	01.07.99
REPLY DUE	**within 3 month(s)** from the above date of mailing

Applicant's or agent's file reference		
P 1130		
International application No. PCT/IB98/01500	International filing date *(day/month/year)* 28/09/1998	Priority date *(day/month/year)* 26/09/1997
International Patent Classification (IPC) or both national classification and IPC H04N1/32		
Applicant DIGITAL COPYRIGHT TECHNOLOGIES AG et al.		

1. This written opinion is the **first** drawn up by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain document cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

3. The applicant is hereby **invited to reply** to this opinion.

   When? See the time limit indicated above. The applicant may, before the expiration of that time limit, request this Authority to grant an extension, see Rule 66.2(d).

   How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

   Also: For an additional opportunity to submit amendments, see Rule 66.4. For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis. For an informal communication with the examiner, see Rule 66.6.

   If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 26/01/2000.

Name and mailing address of the international preliminary examining authority:	Authorized officer / Examiner
European Patent Office D-80298 Munich Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Moorhouse, D Formalities officer (incl. extension of time limits) Mader, D Telephone No. (+49-89) 2399 2887

Form PCT/IPEA/408 (cover sheet) (January 1994)

I. Basis of the opinion

1. This opinion has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed".*):

Description, pages:

1-51 as originally filed

Claims, No.:

1-42 as originally filed

Drawings, sheets:

1/9-9/9 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. This opinion has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been and will not be examined in respect of:

- ☐ the entire international application,
- ☒ claims Nos. 2-17, 20, 22-25, 27, 31-35, 38, 40, 42,

because:

- ☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 2-17, 20, 22-25, 27, 31-35, 38, 40, 42 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

IV. Lack of unity of invention

1. In response to the invitation (Form PCT/IPEA/405) to restrict or pay additional fees, the applicant has:

   ☐ restricted the claims.

   ☐ paid additional fees.

   ☐ paid additional fees under protest.

   ☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied with for the following reasons and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees:

   see separate sheet

3. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this opinion:

   ☒ all parts.

   ☐ the parts relating to claims Nos. .

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	
Inventive step (IS)	Claims	1, 18, 29, 30, 36, 37, 39 : No
Industrial applicability (IA)	Claims	

2. Citations and explanations

   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Concerning Boxes III and VIII

The various definitions of the invention given in independent claims ... are such that the claims as a whole are not clear and concise, contrary to Article 6 PCT. It is thus rendered difficult for third parties to ascertain the extent of protection which is sought, by the Applicant.
The claims should be recast to include only the minimum necessary number of independent claims in any one category, with dependent claims as appropriate (Rule 6.4 (a)-(c) PCT).

This objection is caused in part by the fact that claims 18, 19, 26, 29 and 36 use the formulation "especially for step (b) of claim ..."; claims 30, 39 and 41 use the wording "especially of one of the preceding claims"; and claim 28 uses the wording "preferably as generated in one of claims 25 or (sic) 26". Words such as "especially" and "preferably" are not at all limiting (see International Guidelines, PG-III, 4.6). Thus, claims 18, 19, 26, 28, 29, 30, 36, 39 and 41 must be considered as being independent claims. (Claim 21 is, by any definition, an independent claim).

The fact that said claims are independent results in a plethora of alleged inventions being claimed in the present international application. This results in a lack of unity, as discussed with regard to Box IV below. For the purposes of efficiency, and until the claims have been limited or the aforementioned wording has been removed, the IPEA only intends to examine the independent claims as far as the requirements of Article 33 PCT are concerned, and the first set of claims (1 to 17) as far as the requirements of Article 6 PCT are concerned.

Concerning Box IV

The following document is cited :-

D1 : Delaigle et al.: "Digital Watermarking", Proceedings of the SPIE, Vol. 2659, February 1996, pages 99-110

Comparison of the first alleged invention (claims 1 to 18, 41 and 42) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- encoding a watermark using at least one key of an asymmetric cryptographic key pair,
- encrypting the stego data set using the key pair, and
- transmitting the encrypted stego data set (claim 1 only).

Comparison of the second alleged invention (claims 19 to 38) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- calculating a Fourier transform of at least a part of a cover data set to generate Fourier components,
- modulating at least a part of the Fourier components using a template modulation pattern,
- using an inverse Fourier transform to generate a stego data set,
- calculating a Fourier transform of a possibly scaled and/or rotated version of the stego data set to generate Fourier components thereof,
- calculating a log-polar or log-log transform of these Fourier components,
- calculating the cross-correlation between the log-polar or log-log transform of said modulation pattern and said log-polar or log-log transform of the Fourier components of the stego data set (claim 19 only).

Comparison of the third alleged invention (claims 39 and 40) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- transmitting a hash value of the stego data set to a registration party, and
- storing certification data at the registration party, the certification data comprising a hash value of the stego data set (claim 39).

Thus, the differences between the claims of the different groups of inventions and the disclosure of document D1 are totally different between invention groups. Therefore, the independent claims on file are not linked together by a **single general <u>inventive</u> concept**, as required by Rule 13.1 PCT.

The IPEA has chosen not to invite the Applicant to pay additional examination fees pursuant to Rule 68.1 PCT since, as pointed out above, the lack of unity seems to arise (for the most part) from the choice of claim wording adopted, and could be remedied by appropriate wording amendments.

Concerning Box V

The following further documents are cited :

D2 : EP-A-0 534 419

D3 : Zhao et al: "Embedding Robust Labels into Images for Copyright Protection", Proceedings of the Knowright Conference, Proceedings of The International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technology, 21st August 1995, pages 242-251, XP000603945

D4 : Ruanaidh et al: "Phase Watermarking of Digital Images", Proceedings of The International Conference on Image Processing (IC, Lausanne, Sept. 16th - 19th, 1996, Vol. 3, 16th September 1996, pages 239-242, XP000199952, Institute of Electrical and Electronics Engineers

D5 : FR-A-2 740 897

D6 : EP-A-0 539 726

As pointed out above, a complete examination has not been carried out. Nonetheless, the following objections can already be identified.

<u>Claims 1 and 18</u>
The subject-matter of these independent claims lacks an inventive step with respect to the combination of the disclosures of documents D1 and D2, and therefore does not meet the requirement set out in Article 33 (3) PCT.
Document D1 teaches the skilled person how to watermark digital images using, inter alia, a copyright owner's secret key.

Document D2 teaches the skilled person how to increase cryptographic security by using an asymmetric key pair. It would be obvious to apply the teaching of this document to the teaching of document D1 in order to make it more difficult to infringe the copyright holder's rights, thus arriving at the subject-matter of independent claims 1 and 18. It is further noted here that claim 1 even includes an alternative in which only one of the keys of pair is used, which is even more obvious than using both keys.

Claim 29
The subject-matter of this claim is rendered obvious by the disclosure of document D3, and thus does not meet the requirement set out in Article 33 (3) PCT.
Document D3 teaches the skilled person how to generate a watermark using a Discrete Cosine Transform. This is technically similar to a Fourier transform, and it would be obvious to the skilled reader that the latter transform could be used instead in realising watermarking algorithms described in document D3, thus arriving at the subject-matter of independent claim 29.

Claim 30
The subject-matter of this claim is rendered obvious by the disclosure of document D4, and thus does not meet the requirement set out in Article 33 (3) PCT.
Document D4 teaches the skilled person how to generate a watermark using a Discrete Fourier Transform, by altering, inter alia, the phase components resulting from the application of said transform. It would be obvious to adapt the teaching of document D4 such that the process of independent claim 30, requiring modification of the magnitude components, is carried out.

Claim 36
The subject-matter of this claim is rendered obvious by the disclosure of document D5, and thus does not meet the requirement set out in Article 33 (3) PCT.
Document D5 teaches the skilled person how to add watermark to, for example, a digital audio signal, by splitting the audio signal up into blocks and carrying out a transformation such as a Fourier transformation. It is also mentioned that the technique can be applied to image signals. In this case, it would be obvious to the skilled person to split the image up into three dimensional spatio-temporal blocks which are, per se, known in the art.

Claim 37

The subject-matter of this claim is rendered obvious by the disclosure of any of the documents D3, D4 and D5, and thus does not meet the requirement set out in Article 33 (3) PCT.

Each of these documents teaches the skilled person how to generate a watermark using cover data transformed into the spatial frequency domain. Lapped Orthogonal Transforms are just one of several well known ways of transforming images into the spatial frequency domain, and their use instead of the transforms disclosed in any of the documents D3 to D5 therefore cannot be considered as being of any inventive significance.

Claim 39

The subject-matter of this claim is rendered obvious by the disclosure of document D6, and thus does not meet the requirement set out in Article 33 (3) PCT.

Document D6 teaches the skilled person how to generate a stego data set and transmit it between two parties, whilst registering certification data at a third party. The only difference between this disclosure and the subject-matter of independent claim 39 is the use of a hash function instead of a cryptographic key in the latter. However, such hash functions and their advantages are well known in the art, and their use in the context of the system disclosed in document D6 thus cannot be considered as being of any inventive significance.

Concerning Box VII

The claims are not in the two-part form defined in Rule 6.3 (b) PCT.

The inclusion by reference of the priority document may be objectionable under certain national or regional jurisdictions (e.g. Europe).

The abbreviation "IAD" appearing on page 13, line 33 has not been previously defined.

Concerning Box VIII

Claims 1, 3, 5 to 7, 9, 10, 12 and 13 lack clarity, and therefore do not meet the requirement set out in Article 6 PCT.

Claim 1

This claim is far too vaguely and speculatively worded. It is, for example, not clear from the present claim, how the various levels of security referred to in the description are realised, since only one watermark and only one key need be used, according to certain claimed alternatives. In the case of the other alternatives, i.e. more than one watermark and a second (public) key, it is completely obscure what is done with these items.

From the description it would appear that a detection watermark is embedded, followed by a first layer of cryptographic protection, followed by embedding of a private watermark, followed by more cryptographic protection, followed by embedding of a public watermark and finally a third layer of cryptographic protection (see, in particular, pages 23 and 24).

It is furthermore not clear, whether "encoding" in the claim is the same as "encrypting" in the description.

Moreover, it is not clear how the claimed subject-matter solves the problem set out in the description relating to the copyright holder having to reveal the private key, since one of the claimed alternatives reales to use only of the public key.

Claim 4

There is no support in the description for the features of this claim, in particular pages 30 to 33 (section IIIb) do not mention modulation of the phase components.

Claim 5

There is no support in the description for the features of this claim.

Claim 6

This claim implies, by the use of the word "further", that claim 1 does not require the generation of a first watermark, and thus contradicts claim 1, which clearly specifies such a generation in step (b).

Moreover, it is not clear if "at least a first watermark" means "at least one example of a first type of watermark" or "a first type of watermark, a second type of watermark", etc.

Claim 7

Claim 6 implies that the first watermark is the private watermark (which, according to pages 23 and 24 is encrypted using the private key (ps_H)). Claim 7 then implies that the first (private) watermark is encrypted using a hash value, which contradicts said description pages.

Claim 9

There is no support in the description for more than one second watermark.

Further, this claim contradicts page 24, line 4, according to which the transform is carried out on the **cover** data (CD).

Claim 10

Step (ii) implies that it is possible to use both keys (ps_H and vs_H) can be used as seeds, which contradicts page 31, line 18 of the description.

Claim 12

It is not at all clear from the claim, what "erased elements" might be. Why, and by whom or what have they been erased ?

EPA/EPO/OEB
D-80298 München
+49 89 2399-0
TX 523 656 epmu d
FAX +49 89 2399-4465

Europäisches Patentamt
Eu[illegible]an Pate[illegible] Office
Office européen des brevets

Generaldirektion 2
Directorate General 2
Direction Générale 2

Correspondence with the EPO on PCT Chapter II demands

In order to ensure that your PCT Chapter II demand is dealt with as promptly as possible you are requested to use the enclosed self-adhesive labels with any correspondence relating to the demand sent to the Munich Office.

One of these labels should be affixed to a prominent place in the upper part of the letter or form etc. which you are filing.

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

E. BLUM & Co.
Vorderberg 11
8044 ZÜRICH
SUISSE

27. DEZ. 1999

2
27/12/gp

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

Date of mailing (*day/month/year*)	22. 12. 99
Applicant's or agent's file reference P 1130	**IMPORTANT NOTIFICATION**

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/IB98/01500	28/09/1998	26/09/1997

Applicant
DIGITAL COPYRIGHT TECHNOLOGIES AG et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

   The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

   Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

   For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Stannartz, B Tel.+49 89 2399-8242

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P 1130	**FOR FURTHER ACTION** See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB98/01500	International filing date *(day/month/year)* 28/09/1998	Priority date *(day/month/year)* 26/09/1997
International Patent Classification (IPC) or national classification and IPC H04N1/32		
Applicant DIGITAL COPYRIGHT TECHNOLOGIES AG et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 11 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 7 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand 22/01/1999	Date of completion of this report 22. 12. 99
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Moorhouse, D Telephone No. +49 89 2399 8631

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-8,10-51	as originally filed			
9	as received on	28/08/1999	with letter of	26/08/1999

Claims, No.:

1-22	as received on	28/08/1999	with letter of	26/08/1999

Drawings, sheets:

1/9-9/9	as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☒ the claims, Nos.: 23-42
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

- ☐ restricted the claims.
- ☐ paid additional fees.
- ☐ paid additional fees under protest.

☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

☐ complied with.

☒ not complied with for the following reasons:

see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

☒ all parts.

☐ the parts relating to claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-22
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-17
	No:	Claims	18-22
Industrial applicability (IA)	Yes:	Claims	1-22
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Concerning Box IV

The following document is cited :-

D1 : Delaigle et al.: "Digital Watermarking", Proceedings of the SPIE, Vol. 2659, February 1996, pages 99-110

Comparison of the first alleged invention (claims 1 to 17) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- encoding a watermark using at least one key of an asymmetric cryptographic key pair,
- encrypting the stego data set using the key pair, and
- transmitting the encrypted stego data set.

Comparison of the second alleged invention (claim 18) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- generating at least one message
- digitally signing said message using an asymmetric cryptographic key pair, and
- using the signature as a seed for watermark generation.

Comparison of the third alleged invention (claims 19 and 20) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:
- calculating at least some magnitude Fourier components of a cover data set,
- applying an authentification function to said components to generate an authentification message,
- encrypting the authentification message using a secret key of an asymmetric cryptographic key pair, and
- embedding said encrypted message as a payload in a public watermark.

Comparison of the fourth alleged invention (claims 21 and 22) with the disclosure of document D1 shows that the following technical features could be considered as contributing to the prior art as represented by document D1:

- transmitting a hash value of the stego data set to a registration party, and
- storing certification data at the registration party, the certification data comprising a hash value of the stego data set, a digital time stamp and information designating the originator of the stego data set.

Thus, the differences between the claims of the different groups of inventions and the disclosure of document D1 are totally different between invention groups. Therefore, the independent claims on file are not linked together by a **single general inventive concept**, as required by Rule 13.1 PCT.

The IPEA chose not to invite the Applicant to pay additional examination fees pursuant to Rule 68.1 PCT since, as pointed out above, the lack of unity seemed to arise (for the most part) from the choice of claim wording adopted and the desire to protect subpart of the invention, and could have been remedied by appropriate wording amendments.

Concerning Box V

The following further documents were cited in the Written Opinion :

D2 : EP-A-0 534 419

D3 : Zhao et al: "Embedding Robust Labels into Images for Copyright Protection", Proceedings of the Knowright Conference, Proceedings of The International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technology, 21st August 1995, pages 242-251, XP000603945

D4 : Ruanaidh et al: "Phase Watermarking of Digital Images", Proceedings of The International Conference on Image Processing (IC, Lausanne, Sept. 16th - 19th, 1996, Vol. 3, 16th September 1996, pages 239-242, XP000199952, Institute of Electrical and Electronics Engineers

D5 : FR-A-2 740 897

D6 : EP-A-0 539 726

The following documents are cited for the first time in this Report, following the drafting of certain claims as being indisputably independent :

D7 : Delaigle J.-F. et al: 'Digital Images Protection Techniques in a Broadcast Framework: An Overview', PROCEEDINGS OF THE EUROPEAN CONFERENCE ON MULTIMEDIA APPLICATIONS, SERVICES AND TECHNIQUES, Vol. 2, 28 - 30 May 1996, pages 711-727, XP000199920, Louvain la Neuve (BE)

D8 : Zhao et al: 'A WWW Service to embed and prove digital copyright watermarks' PROCEEDINGS OF THE EUROPEAN CONFERENCE ON MULTIMEDIA APPLICATIONS, SERVICES AND TECHNIQUES, vol. 2, 28 - 30 May 1996, pages 695-709, XP000199921, Louvain la Neuve (BE)

As pointed out with respect to clarity and Box VIII below, various claims lack clarity. Nonetheless, should these clarity objections be met during further prosecution of this application in the national / regional phase, then the comments below regarding inventive step would be applicable.

Claims 1 to 17

The subject-matter of these claims requires that, rather than a single private key, an asymmetric pair of cryptographic keys is used in both generating a watermark and in encrypting the watermarked data. Whilst, as set out in the prior art summary below, both asymmetric key pairs and watermarks using such pairs are known, there is no prior art document which suggests that the same pair be used for watermarking and encrypting the watermarked data set. This would appear to be a step back from what would be the result of a combination of document D7, disclosing the use of asymmetric cryptographic key pairs, with, for example, a document D2 relating to cryptography in general, namely that, for full security, different keys should be used for watermarking and final encryption of the result of watermarking.

Claim 18

The subject-matter of this claim is rendered obvious by the disclosure of document D3, and thus does not meet the requirement set out in Article 33 (3) PCT.

Document D3 teaches the skilled person that a message, relating to features extracted from an image to be watermarked, can be digitally signed using a private key and then used as a seed for watermark generation (in particular, for seeding the positions at which said watermark is inserted) - see the top of page 244. The only difference with respect to the subject-matter of independent claim 18 is the use of an asymmetric cryptographic key pair. Despite the arguments of the Applicant relating to the complexity of such key pairs, the IPEA does not consider that this fact alone would put the skilled person off at least considering using them in place of a private key. Moreover, claim 18 does not specify how the method is adapted to the use of an asymmetric cryptographic key pair. Thus, the subject-matter of claim 18 is derivable in an obvious manner from the disclosure of document D3.

<u>Claims 19 and 20</u>
The subject-matter of these claims is rendered obvious by the disclosure of document D4 taken in combination with the disclosure of any of the documents D1, D3 and D7, and thus does not meet the requirement set out in Article 33 (3) PCT.
Document D4 teaches the skilled person how to generate a watermark using a Discrete Fourier Transform, by altering, inter alia, the phase components resulting from the application of said transform. It would be obvious to adapt the teaching of document D4 such that the process of independent claim 30, requiring modification of the magnitude components, is carried out, particularly since this possibility is also hinted at in the disclosure of document D4.
Moreover, each of the documents D1, D3 and D7 discloses the use of keys in watermarking. Their use to control the insertion of the watermarks disclosed in document D4 is thus an obvious measure to take. The remarks made above with respect to the use of asymmetric cryptographic key pairs are applicable to claim 19 also.

<u>Claims 21 and 22</u>
The subject-matter of these claims is rendered obvious by the disclosure of document D8, and thus does not meet the requirement set out in Article 33 (3) PCT.
Document D8 teaches the skilled person how to generate a stego data set and transmit it between two parties, whilst registering certification data at a third party (see the paragraph labelled (3) at the top of page 705). The only difference between this disclosure and the subject-matter of independent claim 39 is the use of a hash function

instead of a cryptographic key in the latter. However, such hash functions and their advantages are well known in the art, and their use in the context of the system disclosed in document D8 thus cannot be considered as being of any inventive significance.

Concerning Box VII

The claims are not in the two-part form defined in Rule 6.3 (b) PCT.

The inclusion by reference of the priority document may be objectionable under certain national or regional jurisdictions (e.g. Europe).

The abbreviation "IAD" appearing on page 13, line 33 has not been previously defined.

Concerning Box VIII

Claims 1, 4, 6, 7, 12, 18 and 19 lack clarity and/or support in the description, and therefore do not meet the requirement set out in Article 6 PCT.

Claim 1
This claim is far too vaguely and speculatively worded. It is, for example, not clear from the present claim, how the various levels of security referred to in the description are realised, since only one watermark and only one key need be used, according to certain claimed alternatives. In the case of the other alternatives, i.e. more than one watermark and a second (public) key, it is completely obscure what is done with these items. For example, if only one key of a pair is used ("at **least** one" means one, or more than one), is it the private or the public key. In the former case, their is very little difference with respect to certain prior approaches. In the case of two keys, are different watermarks protected differently ?
From the description it would appear that a detection watermark is embedded, followed by a first layer of cryptographic protection, followed by embedding of a private watermark, followed by more cryptographic protection, followed by embedding of a public watermark and finally a third layer of cryptographic protection (see, in particular, pages 23 and 24).

It is furthermore not clear, whether "encoding" in the claim is the same as "encrypting" in the description, as "encoding" is never actually defined in the description.

Claim 4
There is no support in the description for the features of this claim, in particular pages 30 to 33 (section IIIb) do not mention modulation of the phase components.

Claim 6
The wording "encoded" is objected to for reasons set out above with respect to claim 1. It is not clear, where in the description there is support for use of more than one watermark *of the first type.*

Claim 7
Claim 6 implies that the first watermark is the private watermark (which, according to pages 23 and 24 is the type of watermark which is encrypted using the private key (ps_H), whereas the public watermark is encrypted using the public key (vs_H)). Claim 7 then implies that the first (private) watermark is encrypted using a hash value, which contradicts said description pages.

Claim 12
It is not at all clear from the claim, what "erased elements" might be. Why, and by whom or what have they been erased ? The claim per se must define what this wording means.

Claim 18
It is not at all clear what is meant by the wording "generating at least one message", because neither the starting data nor the resulting data is defined.
By analogy with the objections to claim 1, it is not clear, what the public key of the pair is used to encrypt, and what the private key is used to encrypt.

Claim 19
It is not clear what is meant by "calculating *at least* *some* magnitude Fourier components".

It is not clear what an "authentification *value*" is. In line with the description, the wording "an authentification message" should have been used on this claim.

It is not clear from the "embedding" strep, that this step uses the public key.

propose a digital signature scheme for watermarking facsimile documents (binary images). This scheme modify the length of certain runs of data with a single bit of the signature data.

Disclosure of the Invention

It is an object of the present invention to provide a system of the type mentioned above that provides a simple and secure way of generating and transmitting watermarked data. This object is achieved by the methods described in the claims.

In one aspect of the invention, this object is achieved by an integrated solution method for generating and transmitting a data set between two parties H and B comprising the steps of a) providing a cover data set corresponding to the data set to be transmitted, b) generating a stego data set of said cover data set by embedding at least one digital watermark in said cover data set, wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair of H, said key pair comprising a secret private key and a known public key derived therefrom, and c) encrypting said stego data set using said key pair of H, d) transmitting said encrypted stego data set from said party H to said party B.

Preferably, the private and public keys of party H are an elliptic curve key pair.

The party creating the watermark can embed a detection, a private and a public watermark in the data set, wherein the detection or the private watermark is derived from the private key, the public watermark from the public key. The public watermark can be detected by third parties while the private watermark can only be detected using private information. Preferably, the detection or private watermark is not derived from the private key directly but from a hash value of the same and/or from a signature generated with the same, such that the

amended Sheet

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only
International Application No.
International Filing Date
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* P 1130

Box No. I TITLE OF INVENTION Method for generating and verifying digital watermarks and for exchanging data containing digital watermarks

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

Digital Copyright Technologies AG
Stauffacherstrasse 149
CH-8004 Zürich
Switzerland

☐ This person is also inventor.

Telephone No.

Facsimile No.

Teleprinter No.

State *(that is, country)* of nationality: CH

State *(that is, country)* of residence: CH

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

HERRIGEL Alexander
Bergstrasse 62
CH-8702 Meilen
Switzerland

This person is:

☐ applicant only

☒ applicant and inventor

☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: DE

State *(that is, country)* of residence: CH

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

E. Blum & Co.
Vorderberg 11
CH-8044 Zürich
Switzerland

Telephone No. 01/261 54 54

Facsimile No. 01/251 67 17

Teleprinter No. 816 559

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuation of Box No. III **FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)**

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

O'RUANAIDH Joseph J.K.
Studio 11
Rue Jacques Dalphin 11, Carouge
CH-1227 Geneva
Switzerland

This person is:
- [ ] applicant only
- [X] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: IE

State *(that is, country)* of residence: CH

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [X] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

PUN Thierry
60, Chemin de la Gradelle
CH-1224 Chêne-Bougeries
Switzerland

This person is:
- [ ] applicant only
- [X] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: FR

State *(that is, country)* of residence: CH

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [X] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- [ ] applicant only
- [ ] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [ ] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- [ ] applicant only
- [ ] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [ ] the United States of America only
- [ ] the States indicated in the Supplemental Box

- [ ] Further applicants and/or (further) inventors are indicated on another continuation sheet.

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

☒ **AP** **ARIPO Patent: GH** Ghana, **GM** Gambia, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **SD** Sudan, **SZ** Swaziland, **UG** Uganda, **ZW** Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT

☒ **EA** **Eurasian Patent: AM** Armenia, **AZ** Azerbaijan, **BY** Belarus, **KG** Kyrgyzstan, **KZ** Kazakhstan, **MD** Republic of Moldova, **RU** Russian Federation, **TJ** Tajikistan, **TM** Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

☒ **EP** **European Patent: AT** Austria, **BE** Belgium, **CH and LI** Switzerland and Liechtenstein, **CY** Cyprus, **DE** Germany, **DK** Denmark, **ES** Spain, **FI** Finland, **FR** France, **GB** United Kingdom, **GR** Greece, **IE** Ireland, **IT** Italy, **LU** Luxembourg, **MC** Monaco, **NL** Netherlands, **PT** Portugal, **SE** Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☒ **OA** **OAPI Patent: BF** Burkina Faso, **BJ** Benin, **CF** Central African Republic, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroon, **GA** Gabon, **GN** Guinea, **ML** Mali, **MR** Mauritania, **NE** Niger, **SN** Senegal, **TD** Chad, **TG** Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* ....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

- ☒ **AL** Albania
- ☒ **AM** Armenia
- ☒ **AT** Austria
- ☒ **AU** Australia
- ☒ **AZ** Azerbaijan
- ☒ **BA** Bosnia and Herzegovina
- ☒ **BB** Barbados
- ☒ **BG** Bulgaria
- ☒ **BR** Brazil
- ☒ **BY** Belarus
- ☒ **CA** Canada
- ☒ **CH and LI** Switzerland and Liechtenstein
- ☒ **CN** China
- ☒ **CU** Cuba
- ☒ **CZ** Czech Republic
- ☒ **DE** Germany
- ☒ **DK** Denmark
- ☒ **EE** Estonia
- ☒ **ES** Spain
- ☒ **FI** Finland
- ☒ **GB** United Kingdom
- ☒ **GE** Georgia
- ☒ **GH** Ghana
- ☒ **GM** Gambia
- ~~☒ **GW** Guinea-Bissau~~
- ☒ **HR** Croatia
- ☒ **HU** Hungary
- ☒ **ID** Indonesia
- ☒ **IL** Israel
- ☒ **IS** Iceland
- ☒ **JP** Japan
- ☒ **KE** Kenya
- ☒ **KG** Kyrgyzstan
- ☒ **KP** Democratic People's Republic of Korea
- ☒ **KR** Republic of Korea
- ☒ **KZ** Kazakhstan
- ☒ **LC** Saint Lucia
- ☒ **LK** Sri Lanka
- ☒ **LR** Liberia
- ☒ **LS** Lesotho
- ☒ **LT** Lithuania
- ☒ **LU** Luxembourg
- ☒ **LV** Latvia
- ☒ **MD** Republic of Moldova
- ☒ **MG** Madagascar
- ☒ **MK** The former Yugoslav Republic of Macedonia
- ☒ **MN** Mongolia
- ☒ **MW** Malawi
- ☒ **MX** Mexico
- ☒ **NO** Norway
- ☒ **NZ** New Zealand
- ☒ **PL** Poland
- ☒ **PT** Portugal
- ☒ **RO** Romania
- ☒ **RU** Russian Federation
- ☒ **SD** Sudan
- ☒ **SE** Sweden
- ☒ **SG** Singapore
- ☒ **SI** Slovenia
- ☒ **SK** Slovakia
- ☒ **SL** Sierra Leone
- ☒ **TJ** Tajikistan
- ☒ **TM** Turkmenistan
- ☒ **TR** Turkey
- ☒ **TT** Trinidad and Tobago
- ☒ **UA** Ukraine
- ☒ **UG** Uganda
- ☒ **US** United States of America
- ☒ **UZ** Uzbekistan
- ☒ **VN** Viet Nam
- ☒ **YU** Yugoslavia
- ☒ **ZW** Zimbabwe

Check-boxes reserved for designating States (for the purposes of a national patent) which have become party to the PCT after issuance of this sheet:

- ☒ GD Grenada
- ☐ ....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) (26/09/97) 26 September 1997	97 810 708.4		EP	
item (2)				
item (3)				

☐ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s):

* *Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):*

ISA / EP

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority):*

Date *(day/month/year)*	Number	Country *(or regional Office)*
28/08/98 28 August 1998	97810708.4	EP Rijswijk

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets**:

request	:	4
description (excluding sequence listing part)	:	51
claims	:	12
abstract	:	1
drawings	:	9
sequence listing part of description	:	0
Total number of sheets	:	77

This international application is **accompanied by** the item(s) marked below:

1. ☒ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☐ other *(specify)*:

Figure of the drawings which should accompany the abstract: 3

Language of filing of the international application: English

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

E. Blum & Co.
i.V.
[signature]
Paul Ronchi

Zürich, 25 September 1998 rw

For receiving Office use only

1. Date of actual receipt of the purported international application:
2. Drawings: ☐ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:
4. Date of timely receipt of the required corrections under PCT Article 11(2):
5. International Searching Authority (if two or more are competent): ISA /
6. ☐ Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

E. BLUM & CO.
Vorderberg 11
CH-8044 Zürich
SUISSE

21. OKT. 1998

Date of mailing (day/month/year) 15 October 1998 (15.10.98)	
Applicant's or agent's file reference P 1130	**IMPORTANT NOTIFICATION**
International application No. PCT/IB98/01500	International filing date (day/month/year) 28 September 1998 (28.09.98)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 26 September 1997 (26.09.97)
Applicant DIGITAL COPYRIGHT TECHNOLOGIES AG et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.

3. An **asterisk(*)** appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

4. The **letters "NR"** appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
26 Sept 1997 (26.09.97)	97810708.4	EP	14 Octo 1998 (14.10.98)

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland** Facsimile No. (41-22) 740.14.35	Authorized officer Marc Salzman Telephone No. (41-22) 338.83.38

P ENT COOPERATION TREA

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF RECEIPT OF RECORD COPY

(PCT Rule 24.2(a))

To:

E. BLUM & CO.
Vorderberg 11
CH-8044 Zürich
SUISSE

13. OKT. 1998

Date of mailing (day/month/year)	IMPORTANT NOTIFICATION
02 October 1998 (02.10.98)	
Applicant's or agent's file reference	**International application No.**
P 1130	PCT/IB98/01500

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

DIGITAL COPYRIGHT TECHNOLOGIES AG (for all designated States except US)
HERRIGEL, Alexander et al (for US)

International filing date	:	28 September 1998 (28.09.98)
Priority date(s) claimed	:	26 September 1997 (26.09.97)
Date of receipt of the record copy by the International Bureau	:	30 October 1998 (30.10.98)
List of designated Offices	:	

AP :GH,GM,KE,LS,MW,SD,SZ,UG,ZW
EA :AM,AZ,BY,KG,KZ,MD,RU,TJ,TM
EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
OA :BF,BJ,CF,CG,CI,CM,GA,GN,GW,ML,MR,NE,SN,TD,TG
National :AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CU,CZ,DE,DK,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MD,MG,MK,MN,MW,MX,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,UA,UG,US,UZ,VN,YU,ZW

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- [X] time limits for entry into the national phase
- [ ] confirmation of precautionary designations
- [X] requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer: S. Baharlou
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. **It is the applicant's responsibility** to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

The demand must be filed directly with the competent International Preliminary Examining Authority or, if two or more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ EP

PCT

CHAPTER II

DEMAND

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only	
Identification of IPEA	Date of receipt of DEMAND

Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION		Applicant's or agent's file reference P 1130
International application No. PCT/IB98/01500	International filing date *(day/month/year)* (28/09/98) 28 September 1998	(Earliest) Priority date *(day/month/year)* (26/09/97) 26 September 1997
Title of invention METHOD FOR GENERATING AND VERIFYING DIGITAL WATERMARKS AND FOR EXCHANGING DATA CONTAINING DIGITAL WATERMARKS		

Box No. II APPLICANT(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*	
Digital Copyright Technologies AG Stauffacherstrasse 149 CH-8004 Zürich Switzerland	Telephone No.: Facsimile No.: Teleprinter No.:
State *(that is, country)* of nationality: CH	State *(that is, country)* of residence: CH

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*	
Herrigel Alexander Bergstrasse 62 CH-8702 Meilen Switzerland	
State *(that is, country)* of nationality: DE	State *(that is, country)* of residence: CH

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*	
O'Ruanaidh Joseph J.K. Studio 11 Rue Jacques Dalphin 11, Carouge CH-1227 Geneva Switzerland	
State *(that is, country)* of nationality: IE	State *(that is, country)* of residence: CH

[X] Further applicants are indicated on a continuation sheet.

Sheet No. 2.

International application No.
PCT/IB98/01500

Continuation of Box No. II APPLICANT(S)

If none of the following sub-boxes is used, this sheet should not be included in the demand.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

Pun Thierry
60, Chemin de la Gradelle
CH-1224 Chêne-Bougeries
Switzerland

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
FR	CH

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

☐ Further applicants are indicated on another continuation sheet.

Sheet No. 3.

International application No.
PCT/IB98/01500

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The following person is [X] agent [ ] common representative

and [X] has been appointed earlier and represents the applicant(s) also for international preliminary examination.

[ ] is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.

[ ] is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

E. Blum & Co.
Vorderberg 11
CH-8044 Zürich
Switzerland

Telephone No.: 0041 1 261 54 54

Facsimile No.: 0041 1 251 67 17

Teleprinter No.: 816 559

[ ] **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION

Statement concerning amendments:*

1. The applicant wishes the international preliminary examination **to start on the basis of:**

   [X] the international application as originally filed

   the description [ ] as originally filed
   [ ] as amended under Article 34

   the claims [ ] as originally filed
   [ ] as amended under Article 19 (together with any accompanying statement)
   [ ] as amended under Article 34

   the drawings [ ] as originally filed
   [ ] as amended under Article 34

2. [ ] The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.

3. [ ] The applicant wishes the start of the international preliminary examination **to be postponed** until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English

[X] which is the language in which the international application was filed.

[ ] which is the language of a translation furnished for the purposes of international search.

[ ] which is the language of publication of the international application.

[ ] which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

Box No. V ELECTION OF STATES

The applicant hereby elects **all eligible States** *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes **not to elect:**

Sheet No. 4..

International application No.
PCT/IB98/01500

Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:

			For International Preliminary Examining Authority use only: received	not received
1. translation of international application	:	sheets	☐	☐
2. amendments under Article 34	:	sheets	☐	☐
3. copy (or, where required, translation) of amendments under Article 19	:	sheets	☐	☐
4. copy (or, where required, translation) of statement under Article 19	:	sheets	☐	☐
5. letter	:	sheets	☐	☐
6. other *(specify)*	:	sheets	☐	☐

The demand is also accompanied by the item(s) marked below:

1. [X] fee calculation sheet
2. [ ] separate signed power of attorney
3. [ ] copy of general power of attorney; reference number, if any:
4. [ ] statement explaining lack of signature
5. [ ] nucleotide and or amino acid sequence listing in computer readable form
6. [ ] other *(specify)*:

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).

E. Blum & Co.
i.V.

Zürich, 20 January 1999 rw

Rainer Schalch (RA)

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:

2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):

3. [ ] The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. [ ] The applicant has been informed accordingly.

4. [ ] The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.

5. [ ] Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

Replace By Art 34

Claims

1. A method for generating and transmitting a data set between two parties H and B comprising the steps of

a) providing a cover data set (CD) corresponding to the data set to be transmitted,

b) generating a stego data set (SD) of said cover data set (CD) by embedding at least one digital watermark in said cover data set (CD), wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair (ps_H, vs_H) of H, said key pair comprising a secret private key (ps_H) and a known public key (vs_H) derived therefrom,

c) encrypting said stego data set (SD) using said key pair (ps_H, vs_H) of H,

d) transmitting said encrypted stego data set from said party H to said party B.

2. The method of claim 1, wherein said step c) comprises

generating a mask message (B||SN),

generating a signature ($DSSMR_G(ps_H, B||SN)$) of said mask message (B||SN) using said secret private key (ps_H), and

using said signature of said mask message for seeding an encryption algorithm for said stego data set (SD).

3. The method of claim 2 wherein said signature ($DSSMR_G(ps_H, B||SN)$) of said mask message (B||SN) is transmitted from H to B.

4. The method of one of the claims 2 or 3 wherein said encryption algorithm comprises the step of calculating the Fourier transform of said stego data set (SD), modifying the phase components of the Fourier

transform using a pseudo-random pattern seeded by said signature ($DSSMR_G(ps_H, B||SN)$) of said mask message ($B||SN$) and calculating the inverse Fourier transform for generating the encrypted stego data set.

5. The method of one of the preceding claims wherein said key pair (ps_H, vs_H) of H is an elliptic curve key pair.

6. The method of one of the preceding claims wherein said step b) further comprises the step of generating at least a first watermark, wherein said first watermark is encoded using said private key (ps_H) of H.

7. The method of claim 6 wherein said first watermark is encoded using a hash value ($crh(ps_H)$) of said private key (ps_H) and can be decoded by using said hash value ($crh(ps_H)$).

8. The method of claim 6 wherein said first watermark is encoded using a hash value ($crh(OAD_{CD})$) of a signature (OAD_{CD}) generated using said private key (ps_H).

9. The method of one of the preceding claims wherein said step b) further comprises the step of generating at least one second watermark, wherein said second watermark comprises a payload ($pc_H[AM]$) derived from the Fourier transform of said stego data (SD).

10. The method of one of the preceding claims wherein said step b) comprises the steps of:

i) providing a message ($s_1, s_2, \ldots, s_M$) to be transmitted in said at least one watermark, said message consisting of a plurality of symbols,

ii) providing a pseudo random generator seeded with a seed value derived from at least one key of said key pair (ps_H, vs_H) of H or a hash value thereof,

iii) encoding said message using values from said pseudo random generator

iv) using the said encoded message (**m**) for embedding said watermark.

11. The method of claim 10 wherein said step iii) comprises:

for each of said symbols (s_i), generating a pseudo random sequence of numbers (v_1, v_2, ...) by a said pseudo random generator,

using the value of each said symbols (s_i) for selecting a sub-sequence within said pseudo random sequence for forming a symbol vector ($\mathbf{r}_i$), and

adding said symbol vectors ($\mathbf{r}_i$) to generate said encoded message (**m**).

12. The method of claim 11 comprising the following steps for decoding said message:

extracting a read-out message (**m'**) from said watermark, said read-out message being a vector having the same length, if erased elements are replaced by zero, as said symbol vectors ($\mathbf{r}_i$),

generating all possible values of said symbol vectors ($\mathbf{r}_i$) using said pseudo random generator seeded with said seed, and

calculating the cross-correlation between said pseudo random sequences of numbers (v_1, v_2, ...) and said read-out message (**m'**) for retrieving said symbols (s_i).

13. The method of claim 10 wherein said step iii) comprises:

for each bit (b_j) of said symbol sequence (s_1, s_2, ..., s_M), deriving pseudo random vectors ($\mathbf{r}_j^*$)

having elements 1 or -1 from a said pseudo random generator, which pseudo random generator preferably generates m-sequences or Gold codes, and

depending on the value of said bit (b_j), multiplying said pseudo random vector ($\mathbf{r}_j^*$) with +1 or -1 to generate a modified pseudo random vector, and adding said modified pseudo random vectors to generate an encoded message ($\mathbf{m}$).

14. The method of claim 13 comprising the following steps for decoding said message:

extracting a read-out message ($\mathbf{m}'$) from said watermark,

deriving said pseudo random vectors ($\mathbf{r}_j^*$) from said pseudo random generator seeded with a said seed, and

calculating the cross correlation between each of said pseudo random vectors ($\mathbf{r}_j^*$) and said read-out message ($\mathbf{m}'$) for retrieving the corresponding bit (b_j) of the said symbol sequence (s_1, s_2, ..., s_M).

15. The method of one of the claims 10 - 14 wherein the position of components to be modulated by each value of the encoded message ($\mathbf{m}$) is given by a pseudo random generator seeded by a key known by both H and B.

16. The method of one of the preceding claims comprising the step of encoding a message for being embedded in said watermark by using symbol based Reed Solomon codes as error control codes.

17. The method of one of the preceding claims wherein said step b) further comprises the step of calculating a logarithm of said cover data set (CD) before embedding said watermark for embedding said watermark in a perceptually flat domain.

18. A method for generating a stego data set (SD) from a cover data set (CD) especially for step b) of one of the preceding claims, comprising the steps of:

generating at least one message (ID_{CD}),

digitally signing said message (ID_{CD}) using an asymmetric cryptographic key pair (p_H, v_H) and a signature generating algorithm (DSSMR) with message recovery for generating a digital signature (OAD_{CD}), and

generating said stego data set (SD) of said cover data set (CD) by generating at least one digital watermark, wherein said digital signature (OAD_{CD}) is used for deriving a seed for generating said watermark.

19. Method for generating and verifying a watermark in a cover data set (CD) representing a two-dimensional cover image, especially for step b) of one of the preceding claims, comprising the following steps for generating said watermark

A) calculating the Fourier transform of at least part of cover data set (CD) for generating Fourier components of said cover image, and

B) modulating at least part of said Fourier components using a template modulation pattern (**T'**),

C) using the inverse Fourier transform for generating a stego data set (SD),

said method further comprising the following steps for verifying said watermark in a possibly scaled and/or rotated version of said stego data set (SD),

D) calculating the Fourier transform of the possibly scaled and/or rotated version of said stego data set (SD) for generating Fourier components of said stego data set,

E) calculating a log-polar or log-log transform of said Fourier components of said stego data set (SD), and

F) calculating the cross correlation between a log-polar or log-log transform (**T**) of said modulation pattern (**T'**) and said log-polar or log-log transform of said Fourier components of said stego data set for evaluating a scaling and/or rotation factor.

20. The method of claim 19 wherein said step B) further comprises the steps of

calculating a log-polar or log-log transform of said components of said cover data set for generating log-polar components,

modulating said log polar components using a log-polar or log-log transform (**T**) of said modulation pattern (**T'**).

21. A method for verifying a watermark in a possibly rotated and/or scaled version of a two or three dimensional stego data set (SD), comprising the steps of:

A) calculating a Fourier transform of said stego data set (SD),

B) calculating a log-polar or a log-log transform of said Fourier transform of said stego data set,

C) calculating the correlation between said log-polar or log-log transform and a template (**T**), which template is the log-polar or log-log transformation of said watermark.

22. The method of claim 21, wherein said step B) comprises the step of calculating the log-polar transform of said Fourier transform of said stego data set and said step C) comprises a step of detecting a rotation and either a uniform scaling suffered by said stego data set or a ratio between block size used in embedding and extraction of said watermark.

23. The method of claim 21, wherein said step B) comprises the step of calculating the log-log transform of said Fourier transform of said stego data set and said step C) comprises a step of detecting either a change in aspect ratio suffered by said stego data set or a change of aspect ratio between block sizes used in embedding and extraction of said watermark.

24. The method of claim 21, wherein the presence of said watermark is verified by means of a Bayesian approach to detect the presence of said watermark given a said key without decoding said watermark.

25. The method of one of the claims 21 - 24, further comprising at least one of the following steps:

i) pre-filtering said cover data by applying a windowing algorithm thereto, preferably Blackman, Hanning or Welch windowing, and/or

ii) calculating the variance or distribution of the Fourier transform locally for filtering outliers and noise, and/or

iii) locating local peaks in said Fourier transform and carrying out said step B) for these local peaks only, preferably transforming only the coordinates of these local peaks, and preferably using the log-log or log-polar transform of said coordinates for calculating said correlation,

iv) excluding low frequency data from said Fourier transform before carrying out said step B), and/or,

v) detecting a scaling and/or rotation in said step C), using said scaling and/or rotation for either a) scaling and/or or rotating said Fourier transform, calculating a scaled and/or rotated log-log or log-polar transform therefrom and correlating said rotated log-log or log-polar transform with said template, or b) calculating a second template by scaling and/or rotating

an original Fourier-space template and calculating a log-log and or log-polar transform therefrom and using said second template for calculation a second correlation with said log-log or log-polar transform of said stego data, and/or

vi) weighing low frequency components of said log-log or log-polar transform stronger that high frequency components while carrying out said correlation.

26. A method for generating a stego data set (SD) from a cover data set (CD) especially for step b) of one of the claims 1 - 18, comprising the step of modulating said cover data set (CD) using a given pattern, which pattern is calculated from a watermark using the following steps:

A) providing said watermark,

B) calculating a first inverse Fourier transform of said watermark,

C) calculating an inverse log-log or log-polar transform of said watermark, and

D) calculating said pattern from said inverse log-log or log-polar transform.

27. The method of claim 26 further comprising the step of combining the magnitude components of said first inverse Fourier transform with the phases of a Fourier transform of said stego data (SD) to generate a frequency space pattern and, preferably, calculating a second inverse Fourier transform of said frequency space pattern.

28. A method for verifying a watermark in a possibly rotated and/or scaled version of a two or three dimensional stego data set (SD), preferably as generated in one of the claims 25 or 26, comprising the steps of:

A) calculating a first Fourier transform of said stego data set (SD),

B) calculating a log-polar or a log-log transform of said Fourier transform of said stego data set,

C) calculating a second Fourier transform of said log-polar or log-log transform and searching said watermark in said second Fourier transform.

29. A method for generating a watermark in a cover data set (CD) representing a two or three dimensional data set, especially for step b) of one of the preceding claims, comprising the following steps:

A) generating a template modulation pattern (**T'**) using a random number generator seeded by a key (K),

B) calculating the Fourier transform of at least part of said cover data set (CD) for generating Fourier components of said cover data set,

C) modulating at least part of said Fourier components using said template modulation pattern (**T'**),

D) using the inverse Fourier transform for generating a stego-image.

30. Method for generating a watermark in a cover data set (CD) representing a cover image especially for one of the preceding claims, characterized by the step of dividing said image into a plurality of blocks and by the following steps carried out for each block:

i) calculating the Fourier transform of the block,

ii) modulating at least part of the magnitude components of the Fourier transform of the block using a modulation pattern, which modulation pattern defines values to be added/subtracted to/from said magnitude components, wherein for each magnitude component its corresponding phase component determines if said value is to be added or subtracted, and wherein the same modulation pattern is used for all blocks.

31. The method of claim 30 wherein said blocks are adjacent.

32. The method of claim 30 wherein the said image is divided into a plurality of overlapping blocks and wherein the step i) comprises calculating the Lapped Orthogonal transform of each block to embed a Lapped Orthogonal transform based watermark.

33. The method of claim 30 wherein the said image is divided into a plurality of non-square blocks and wherein the step i) consists in padding each block with appropriate values (constant or symmetric extension) in order to obtain square blocks, calculating the Fourier transform of each obtained square block to embed Fourier transform based watermark.

34. The method of claim 30 wherein the said image is divided into a plurality of non-square blocks and wherein said step i) comprises computing the arbitrary length wavelet transform of each block to embed a wavelet transform based watermark.

35. The method of one of the claims 30 - 34 wherein the watermark is applied to all or some of the frames of a video.

36. A method for generating a stego data set (SD) from a cover data set (CD) especially for step b) of one of the claims 1 - 18, by adding a watermark to said cover data set, wherein said cover data set comprises video data, comprising the steps of

generating three dimensional spatio-temporal blocks of said video data and

applying said watermark to each of said blocks, preferably by calculating a Fourier transform of each of said blocks.

37. A method for generating a stego data set (SD) from a cover data set (CD) especially according to one of the preceding claims, by adding a watermark to said cover data set comprising the steps of

dividing said stego data sets into blocks,

calculating a lapped orthogonal transform (LOT) of each of said blocks, and

applying said watermark to said lapped orthogonal transforms.

38. The method of claim 37 further comprising the step of modulating selected components of said lapped orthogonal transform (LOT) as a function of a local image characteristics, such as the local image variance.

39. Method for generating and transmitting a data set between two parties H and B, especially of one of the preceding claims, comprising the steps of

providing a cover data set (CD) corresponding to the data set to be transmitted,

generating a stego data set (SD) of said cover data set (CI) at a party H by generating at least one digital watermark in said cover data set (CD),

transmitting a hash value of said stego data set (SD) to a registration party (O), and

permanently storing certification data (CCD) at said registration party (O), said certification data comprising said hash value of said stego data set (SI), a digital time stamp (TVP) and information designating said party H.

40. The method of claim 39 further comprising the steps of generating a digital signature of said certification data (CCD) using an asymmetric cryptographic key pair (ps_O, vs_O) of said registration party (O), transmitting said certification data (CCD) and said digi-

tal signature to said party H, and verifying said digital signature at said party H by using a public key (vs_O) of said key pair of said registration party.

41. A method for embedding a watermark in a cover data set for generating a stego data set, especially of one of the preceding claims, comprising the steps of

calculating at least some magnitude Fourier components (MC) of said cover data set (CD),

applying an authentication function (AF) for generating a value (AM) derived from said Fourier components (MC),

ciphering said value (AM) using a secret key (pc_H) of an asymmetric key pair (pc_H, vc_H) for generating a ciphered message, and

embedding said ciphered message as a payload in a public watermark.

42. A method for verifying the originality of a possibly modified stego data set generated with the method of claim 41 comprising the step of reading said value (AM) by decoding said ciphered message using the public key of said key par and comparing said magnitude Fourier components to said stego data set.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 1/32, 7/26	A1	(11) International Publication Number: **WO 99/17536** (43) International Publication Date: 8 April 1999 (08.04.99)

(21) International Application Number: PCT/IB98/01500

(22) International Filing Date: 28 September 1998 (28.09.98)

(30) Priority Data:
97810708.4 26 September 1997 (26.09.97) EP

(71) Applicant *(for all designated States except US)*: DIGITAL COPYRIGHT TECHNOLOGIES AG [CH/CH]; Stauffacherstrasse 149, CH-8004 Zürich (CH).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HERRIGEL, Alexander [DE/CH]; Bergstrasse 62, CH-8702 Meilen (CH). O'RUANAIDH, Joseph, J., K. [IE/CH]; Studio 11, 11, rue Jacques Dalphin, CH-1227 Carouge (CH). PUN, Thierry [FR/CH]; 60, chemin de la Gradelle, CH-1224 Chêne-Bougeries (CH).

(74) Agent: E. BLUM & CO.; Vorderberg 11, CH-8044 Zürich (CH).

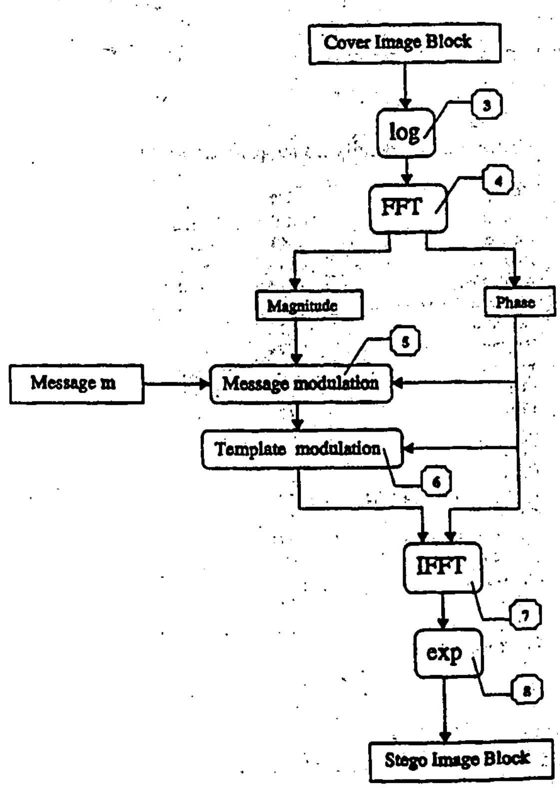
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR GENERATING AND VERIFYING DEGITAL WATERMARKS AND FOR EXCHANGING DATA CONTAINING DIGITAL WATERMARKS

(57) Abstract

A method for generating digital watermarks and for exchanging data containing such watermarks is described. It is based on a watermarking technique which is robust against image transformation techniques such as compression, rotation, translation, scaling and/or change of proportion. It uses modulation of the magnitude components in Fourier space and adds/reads a template in the log-polar or log-log transform of the magnitude components. The template is used for analyzing scaling and rotation or change of proportion. In addition, the system applies cryptographic protocols and public key techniques for both, encoding the watermark and transferring watermarked data. Preferably, an author (CH) encodes the watermark using an asymmetric cryptographic key pair provided by a public key infrastructure (PKI) and registers the watermarked data at a trusted registration party (CCC) before transmitting the data to a receiving party (B). The latter can use the public key infrastructure (I) for verifying autorship. Data exchanged by the parties are encrypted using the cryptographic keys. In addition, image (video) originality verification is supported by the same asymmetric key pair as for content protection and for copyright protection.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

Method for generating and verifying digital watermarks and for exchanging data containing digital watermarks

Cross References to Related Applications

This application claims the priority of European patent application 97810708.4, filed Sept. 26, 1997, the disclosure of which is incorporated herein by reference in its entirety.

Technical Field

The present invention relates to methods for generating and verifying digital watermarks and for transmitting data containing digital watermarks according to the preamble of the independent claims.

Background Art

Digital watermarking is a method for marking data sets, such as images, sound or video. A digital watermark consists of a slight modification of the data set that does not affect the data set's usability but that can be detected using dedicated analysis software or apparatus. Watermarking can e.g. be used for marking authorship or ownership of a data set. It can also be applied for verifying the originality of the multimedia data content, where the loss of originality refers to the degree of contents modification suffered by the image.

Digital watermarking can be seen as a fundamental-problem in digital communications (see e.g. I. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum communication for multimedia", Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996). Early methods of encoding watermarks consisted of no more than increment-

ing an image component to encode a binary '1' and decrementing to encode a '0' (G. Caronni "Assuring Ownership Rights for Digital Images" in H. H. Brueggemann and W. Gerhardt-Haeckl, editors, Reliable IT Systems VIS '95, Vieweg Publishing Company, Germany, 1995). Tirkel et al. (A. Z. Tirkel, G. A. Rankin, R. G. van Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne, "Electronic watermark", in Dicta-93, pages 666-672, Macquarie University, Sydney, December 1993) and van Schyndel et al. (A. Z. Tirkel, R. G. van Schyndel, and C. F. Osborne, "a two-dimensional digital watermark", in ACCV'95, pages 378-383, University of Queensland, Brisbane, December 6-8 1995) have applied the properties of m-sequences to produce oblivious watermarks resistant to filtering, cropping and reasonably robust to cryptographic attack. Matsui and Tanaka (K. Matsui and K. Tanaka, "Video-Steganography : How to secretly embed a signature in a picture", in IMA Intellectual Property Project Proceedings, pages 187-206, January 1994) have applied linear predictive coding for watermarking. Their approach to hiding a watermark is to make the watermark resemble quantization noise. Tirkel and Osborne (see above) were the first to note the applicability of spread spectrum techniques to digital image watermarking. Since then there has been an increasing use of spread spectrum in digital watermarking. It has several advantageous features, such as cryptographic security (see Tirkel and Osborne, above), and is capable of achieving error free transmission of the watermark near or at the limits given by the maximum channel capacity (J. Smith and B. Comiskey, "Modulation and information hiding in images", in Ross Anderson, editor, Proceedings of the First International Workshop in Information Hiding, Lecture Notes in Computer Science, pages 207-226, Cambridge, UK, May/June 1996, Springer). Fundamental information theoretic limits to reliable communication have been discussed by some authors (see Smith and Comiskey, above). The shorter the

payload of a watermark, the better are the chances of it being communicated reliably. Spread spectrum is an example of a symmetric key cryptosystem (B. Schneier, "Applied Cryptography", Wiley, 2nd edition, 1995). System security is based on proprietary knowledge of the keys (or pseudo random seeds) which are required to embed, extract or remove an image watermark. One provision in the use of a spread spectrum system is that it is important that the watermarking be non-invertible because only in this way can true ownership of the copyright material be resolved (S. Craver, N. Memon, B. Yeo, and M. Yeung, "Can invisible marks resolve rightful ownership's ?", IS&T/SPIE Electronic Imaging '97 : "Storage and Retrieval of Image and Video Databases", 1997). Ó Ruanaidh et al. (J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Phase watermarking of images", IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996) and Cox et al. (see above) have developed perceptually adaptive transform domain methods for watermarking. In contrast to previous approaches listed above the emphasis was on embedding the watermark in the most significant components of an image or a video frame. The general approach used in these papers is to divide the image into blocks. Each block is mapped into the transform domain using either the Discrete Cosine Transform (W. B. Pennebaker and J. L. Mitchell, "JPEG Still Image Compression Standard", Van Nostrand Reinhold, New York, 1993), the Hadamard Transform (W. G. Chambers, "Basics of Communications and Coding", Oxford Science Publications. Clarendon Press Oxford, 1985) or the Daubechies Wavelet Transform (W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery, "Numerical Recipes in C", Cambridge University Press, second edition, 1992). The phase component of the image or video frame is then modified according to the pseudo-random sequence containing the watermarking information.

Information can be embedded using the DCT (J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection", IEEE Proceedings on Vision, Image and Signal Processing, 143(4) :250-256, August 1996, based on the paper of the same title at the IEEE Conference on Image Processing and Its Applications, Edinburgh, July 1995) FFT magnitude, and phase, Wavelets (see refs. of Ruanaidh, Dowling and Boland, above), Linear Predictive Coding (see Matsui et al., above) and fractals (P. Davern and M. Scott, "Fractal based image steganography", in Ross Anderson, ed., Proceedings of the First International Workshop in Information Hiding, Lecture Notes in Computer Science, pp. 279-294, Cambridge, UK, May/June 1996, Springer Verlag).

The key to making watermarks robust has been the recognition that in order for a watermark to be robust it must be embedded in the perceptually significant components of the image (see ref. of Ruanaidh, Dowling and Boland, and ref. of I. Cox, J. Killian, T. Leighton, and T. Shamoon above). Objective criteria for measuring the degree to which an image component is significant in watermarking have gradually evolved from being based purely on energy content (see refs. of Ruanaidh et al., Cox et al. above), to statistical (see I. Pitas, "A method for signature casting on digital images", Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996) and psychovisual (see J.F. Delaigle, C. De Vleeschouwer, B. Macq, "Digital watermarking", Proceedings of the SPIE Electronic Imaging: Science and Technology, vol. 2659: Optical Security and counterfeit Deterrence Techniques, San Jose, February 1996 and M.D. Swanson, B. Zhu and A. Tewfik, "Transparent robust image watermarking", Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996).

The industrial importance of digital watermarking has resulted in a number of products on the mar-

ket, either based on spread spectrum techniques or additional registration services. They include the Picturemarc system by Digimarc (RHOADS, B. Geoffrey, Digimarc Corp (US), "Steganography Systems, WO 96/36163 A, Sure-Sign (former FBI's Fingerprint) by HighWater Signum (WO 96/27259), IP_2 system by Intellectual Protocols, the Argent system by Digital Information Commodities Exchange, the PixelTag system by the MIT Media Lab, the SysCop system from Zhao and Koch by the Fraüenhofer-Institut für Graphische Datenverarbeitung (J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection", Proceedings of the International Congress on Intellectual Property Rights For Specialized Information, Knowledge and New Technology, August 1995 J. Zhao, "A WWW Service To Embed And Prove Digital Copyright Watermarks", Proc. Of the European Conference on Multimedia Application, Services and Techniques, vol. 2, Louvain-La-Neuve, Belgium, May 1996), and the Tigermark system from NEC (European patent Application EP 766468A, Nippon Electric Corporation (NEC), April 1997)

The approach proposed by Digimarc (see WO 96/36163) adds or subtracts small random quantities from each pixel according to the least significant bit of each pixel compared with the binary mask. The originality of their approach consists in the use of "subliminal digital graticules" that will help in recovering a rotation R and a scaling S performed on the marked image. They use an exhaustive search strategy based on these graticules to recover R and S. This stands in contrast to the template embodiment described here, where the use of log-polar or log-log mapping of the Fourier transform of the image combined with cross-correlation in the log-polar or log-log plane avoid such a search.

The Highwater approach (WO 96/27259) describe a permutation technique to modify the values of the data elements according to certain rules which depend on the message.

The approach of Zhao and Koch, based on the JPEG image compression algorithm, proceeds by segmenting the image into individual 8 x 8 blocks. Only eight coefficients occupying particular positions in the 8 x 8 block of DCT coefficients can be marked. These comprise the low frequency components of the image block but exclude the mean value coefficient as well as the low frequencies. Three of the remaining DCT coefficients are selected using a pseudo random number generator to convey information. The resemblance of this technique to frequency hop spread spectrum communications is also mentioned and the blocks are placed at random positions in the image. A WWW registration service has been proposed for a local registration and a local watermarking, for a server registration and a server watermarking, and for a local watermarking and a server registration. The approach is based on a trusted third party model (WWW server and Watermark Embedding Gateway). This model requires from the Copyright Holder the transfer of relevant confidential information applied for the watermarking process. It is, therefore, possible that the owner of the trusted third party system may impersonate the Copyright Holder and infringe his copyright. Since the applied key for the embedding is not a cryptographic key, copyright protection and communication security are addressed by two different technical solutions, namely the SysCop system and the s-http protocol. These two technical solutions are applied independently. There is no third party verification procedure supported which allows the verification of the seed, applied for the embedding of the watermark, by independent parties, such as a court of law. The s-http protocol (SSL security protocol) differs from the protocol presented below in many aspects (for example, the non-repudiation security service is not supported by the s-http protocol). The keys applied for the embedding of the mark are furthermore not registered in the SysCop system. For copyright verification, the Copy-

right Holder has to disclose his key. The information generated by the trusted third party is based on the cover data, but not on the stego data.

I. Cox et al from NEC (see EP 766 468, above) propose to insert watermark into the perceptually significant components of a decomposition of the data in a manner so as to be visually imperceptible. In contrast to the method described here, they need the original data which is compared to the watermarked data to obtain an extracted watermark.

J.-F. Delaigle at al. (J.-F. Delaigle, J.-M. Boucqueau, J.-J. Quisquater and B. Macq, "Digital Images protection techniques in a broadcast framework: An overview", Proceedings of the European Conference on Multimedia applications, Services and Techniques, vol. 2, Louvain-La-Neuve, Belgium, May 1996, J.-F. Delaigle, C. De Vleeschouwer & B. Macq, "Digital Watermarking", Proceedings of the SPIE, vol. 2659, 1 February 1996) have applied signature labeling techniques for the copyright protection of digital images. The approach presented is very similar a EDI security standards. The labeling does not influence the multimedia data. Their approach is based on an enhanced image format and generates a digital signature label in front of the image. This signature label can be easily overwritten or destroyed. The registration entity supports no secure on-line communication protocol and is constrained by a legal trusted third party. In addition, no means are provided to resolve a conflict if multiple watermarks have been embedded in the same image. In an enhanced architecture they propose a general watermarking function which uses the output of a hash function as the payload of the watermark. This watermark function does not support third party verification and is not based on a spread spectrum technique. In addition, different types of watermarks are not supported. The masking scheme presented depend on a ciphering function for the inscription. In contrast to the approach pre-

sented in this disclosure, the secret key has to be revealed for copyright verification and no coding/decoding along with cryptographic digital signatures are applied. In addition, the cryptographic key applied is only used for ciphering and not for other functional purposes relevant for copyright protection as defined in this disclosure.

S. Matyas at all (Stephen M. Matyas, Donald B. Johnson, An V. Lee, Rostislaw Prymak, William C. Martin, William S. Rohland, and John D. Wilkins, "EP 0 534 419 A", Stephen M. Matyas, Donald B. Johnson, An V. Lee, Rostislaw Prymak, William C. Martin, William S. Rohland, and John D. Wilkins, "EP 0 539 726 A") have specified a system which is based on an architecture with two different entities, namely the data processor with a cryptographic system and the network certification center. The overall system security depends on a hierarchical cryptographic key scheme and digital certificates are only generated for a specific data set, called control vectors. These control vectors set up the basis to identify the access rights of users and associated processes they have initiated. The main focus of the specified system is the enforcement of a dedicated security policy which is based on a hierarchical role model. The system is based on a hardware based security processors and applies symmetric and asymmetric cryptographic keys. The cryptographic protocols applied are different to the protocols presented in this disclosure. The emphasis is to provide a method for controlling the use of private and public keys which is not the purpose of our system. In addition, one entity needs several different types of keys (symmetric and asymmetric) in contrast to our approach which uses for one entity one asymmetric key pair only.

Tanaka et al. (K. Tanaka and K. Matsui, "A Digital Signature scheme on a Document for MH Facsimile Transmission", Electronics & Communications in Japan, Part I - Communications, Vol. 74, No. 8, August 1991)

propose a digital signature scheme for watermarking facsimile documents (binary images). This scheme modify the length of certain runs of data with a single bit of the signature data.

Disclosure of the Invention

It is an object of the present invention to provide a system of the type mentioned above that provides a simple and secure way of generating and transmitting watermarked data. This object is achieved by the methods described in the claims.

In one aspect of the invention, this object is achieved by an integrated solution method for generating and transmitting a data set between two parties H and B comprising the steps of a) providing a cover data set corresponding to the data set to be transmitted, b) generating a stego data set of said cover data set by embedding at least one digital watermark in said cover data set, wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair of H, said key pair comprising a secret private key and a known public key derived therefrom, and c) encrypting said stego data set using said key pair of H, d) transmitting said encrypted stego data set from said party H to said party B.

The party creating the watermark can embed a detection, a private and a public watermark in the data set, wherein the detection or the private watermark is derived from the private key, the public watermark from the public key. The public watermark can be detected by third parties while the private watermark can only be detected using private information. Preferably, the detection or private watermark is not derived from the private key directly but from a hash value of the same and/or from a signature generated with the same, such that the

author of the watermark does not have to reveal his private key if the private watermark is to be verified.

In another aspect of the invention, the cover data set is provided with a digital watermark and derived stego data then securely transmitted to a registration party that permanently stores at least time information, origin of the stego data set, and a digital copyright certificate.

In another aspect of the invention, a template modulation pattern is added to the Fourier transform of an image that is to be provided with a watermark. For checking the watermark, the Fourier transform of the stego-image is calculated. From this Fourier transform, the log-polar mapping transform is generated, which is then searched for the modulation pattern. Using the log-polar transform of the Fourier transform has the advantage that scaling and rotation of the stego-image are expressed in translations. This allows an easy search for rotation and scaling using cross-correlation techniques.

However, especially for video data, a change of proportion (different horizontal and vertical scaling) is more probable than a rotation. In such cases, the template modulation pattern is rather searched in the log-log transform of the Fourier transform. Similarly to the log-polar map, the log-log map allows to express the horizontal scaling and vertical scaling in translations and cross-correlation techniques can be applied to search the template.

In still another aspect of the invention, the image to be watermarked is divided into blocks and the magnitude components of the Fourier transform of each block is modulated using the same pattern. This method provides robustness against cropping of the stego-image because a cropping leads to a circular translation in each block. Preferably, the magnitude components of the Fourier transform are modulated, wherein the sign of the modulation should be derived from the phase components.

thereby reducing interference between the image data and the watermark as explained in the following disclosure.

In a further aspect, the invention consists of a method for generating and transmitting a data set between two parties H and B comprising the steps of providing a cover data set corresponding to the data set to be transmitted, generating a stego data set of said cover data set at a party H by generating at least one digital watermark in said cover data set, transmitting a has value of said stego data set to a registration party, and permanently storing certification data at said registration party, said certification data comprising said hash value of said stego data set, a digital time stamp and information designating said party H.

In a further aspect, the invention relates to a method for generating a stego data set from a cover data set by adding a watermark to said cover data set comprising the steps of dividing said stego data sets into blocks, calculating a lapped orthogonal transform of each of said blocks, and applying said watermark to said lapped orthogonal transforms.

In another aspect, the invention relates to a method for generating a watermark in a cover data set (CD) representing a two or three dimensional data set, especially for step b) of one of the preceding claims, comprising the following steps: A) generating a template modulation pattern (**T'**) using a random number generator seeded by a key (K), B) calculating the Fourier transform of at least part of said cover data set (CD) for generating Fourier components of said cover data set, C) modulating at least part of said Fourier components using said template modulation pattern (**T'**), D) using the inverse Fourier transform for generating a stego-image

The invention further relates to a method for verifying a watermark in a possibly rotated and/or scaled version of a two or three dimensional stego data set, comprising the steps of: A) calculating a Fourier trans-

form of said stego data set (SD), B) calculating a log-polar or a log-log transform of said Fourier transform of said stego data set, and C) calculating the correlation between said log-polar or log-log transform and a template (**T**), which template is the log-polar or log-log transformation of said watermark.

Brief Description of the Drawings

The invention will be better understood and objects other than those set forth above will become apparent when consideration is given to the following detailed description thereof. Such description makes reference to the annexed drawings, wherein:

Fig. 1 the parties involved in individual watermark protection,

Fig. 2 the parties involved in watermark protection using registered cryptographic keys,

Fig. 3 the parties involved in watermark protection using registered cryptographic keys and a registration party,

Fig. 4 the steps taken for embedding a watermark,

Fig. 5 the steps for generating the template,

Fig. 6 the steps for reading a watermark,

Fig. 7 the steps for reading the template,

Fig. 8 the steps for embedding watermark in a rotation, scale and translation invariant domain,

Fig. 9 the steps for embedding the watermark in an image avoiding to map the original image into the rotation, scale and translation invariant domain,

Fig. 10 the steps to extract the watermark from the image,

Fig. 11 the tiling of the watermark in a stego-image or stego video frame, and

Fig. 12 the tiling of the watermark in a cropped stego-image or cropped stego video frame.

Modes for Carrying Out the Invention

I. Terms and Symbols:

Before describing a preferred method and apparatus according to the invention, some key terms and symbols used in its description are explained in the following:

"Image": An image in either digital or physical form which may constitute a still image or a video frame. It can also refer other types of data, such as video and sound, in particular when being used within the context of the protection and owner authentication methods of section II of the disclosure.

"Signal": A signal in either digital or physical form. It may refer to one dimensional or multi-dimensional signals such as image and video.

"Copyright Holder (CH)": A party (or a process acting on behalf of it) "owning" a digital image or video. This is the party that generates the watermarks.

"Buyer (B)": A party (or a process acting on behalf it) which obtains (e.g. by purchase) via electronic means a specific image from the CH.

"Stego": Implies that an image or video data is marked. The stego image is also referred to as the stego data set (e.g. stego image or video frame).

"Cover": Implies that an image or data is unmarked. The cover image is also referred to as the cover data set (e.g. cover image or video frame).

"Watermark": The form the IAD takes when it is in a form suitable for embedding in a signal.

"Copyright Certificate Center (CCC)": An organization (or a process which acts on behalf of it) which registers copyright ownership for a specific image

or video. Successful registration is only based on a sender verification procedure. After successful registration a digital copyright certificate can be generated. The CCC does not act as trusted third party in our system.

"Digital copyright certificate": Digital copyright data which comprise the copyright certificate data and a digital signature.

"Copyright Request Data (CRD)": Copyright data which contains the stego-image, the image ID of the cover-image, a Universal Copyright Convention Notice, a Copyright Symbol, the term ''Copyright'', the year of the copyright, the name of the copyright holder, and the phrase ''All Rights Reserved''.

"Copyright Certificate Data (CCD)": Copyright data which contains relevant copyright information.

"Digital signature": A data string which has been generated by a cryptographic digital signature generation transformation.

"Digital signature generation transformation": A method for producing a digital signature.

"Digital signature verification transformation": A method for verifying whether a digital signature is authentic or not.

"Digital signature scheme": A scheme based on asymmetric cryptographic techniques whose private transformation is used for the digital signature generation and whose public transformation is used for the digital signature verification.

"Digital signature scheme with message recovery": A digital signature scheme for which a priori knowledge of the input data is not required for the signature verification transformation.

"Digital signature scheme with appendix": A digital signature scheme for which the input data is required as input to the digital signature verification transformation.

"Asymmetric key pair": A pair of related cryptographic keys where the private key defines the private transformation and the public key defines the public transformation.

"Symmetric key": A cryptographic key used with a symmetric cryptographic technique and known only to a set of specified entities.

"Public Key Infrastructure (PKI)": An organization (or processes which acts on behalf of it) which offers services for the generation, registration, certification, distribution, validation, and revocation of a certificate associated with an asymmetric key pair.

"Public watermark": A watermark that can be detected using a publicly available key (or a hash value thereof).

"Private watermark": A watermark that can only be detected using a secret key (or a hash value thereof) and some data associated to specific cover data. It is not possible for an unauthorized third party to overwrite or delete the private watermark without the cryptographic secret keying information.

"Detection watermark": A watermark that can only be detected using a secret key (or a hash value thereof). It is not possible for an unauthorized third party to overwrite or delete the private watermark without the cryptographic secret keying information.

"Payload": The core of the hidden IAD in bit form without error control coding applied.

"Image ID": The following format scheme for a globally unique ID: The first 3 bytes determine the CCC, the following 3 bytes determine the CH ID defined by the CCC. Finally the CH can freely assign last 4 bytes for each one of his digital images or videos.

"Oblivious": A watermarking technique which does not require the cover-image for extracting the mark. In other words, only the stego-image is required to extract the mark when using an oblivious marking scheme.

"Template": A hidden message encoded in the image. Two kind of templates are used: "RST template (Rotation-Scale Template)" and "PST template" (Proportion-Scale Template). By detecting the RST template, the scaling (zooming) and rotation suffered by a stego-image can be determined. By detecting the PST template, the horizontal and the vertical scaling are detected, and therefore the change of proportion suffered by a stego-image can be determined.

"Pseudo random seed": A value used to initialize a pseudo random number generator.

"Modulation": Changing a component's value e.g. by addition or multiplication.

Symbols:

H, C, B, I

Distinguished (unique) name of the Copyright Holder, the Copyright Certificate Center, the Buyer B and the Public Key Infrastructure I.

Cert H, Cert C, Cert B

Entity H's public key certificate from I, entity C's public key certificate from I and entity B's public key certificate from I.

(ps_X, vs_X)

The asymmetric signature and verification key pair of an entity with the distinguished name X.

(pc_X, vc_X)

The asymmetric decipherment and encipherment key pair of an entity with the distinguished name X.

CC

A copyright certificate

$DSSMR_G(X,Y,Z)$

A digital signature generation scheme with message recovery, where X denotes the private key, Y the input data, and Z the resulting signature.

$DSSMR_V(X,Y,Z)$

A signature verification scheme with message recovery, where X denotes the public key, Y the input data, and Z the resulting output data.

$DSSAP_G$(X,Y,Z)

A digital signature generation scheme with appendix, where X denotes the private key, Y the input data, and Z the resulting signature.

$DSSAP_V$(X,Y,Z)

A signature verification scheme with appendix, where X denotes the public key, Y the input data, and Z the resulting output data.

crh A collision resistant hash function

OWEA(X,Y,CD, SD)

The oblivious, spread spectrum based watermark embedding algorithm with the seed X, the payload Y, the cover data CD, and the resulting stego data SD.

OWVA(X,SD,Y)

The oblivious, spread spectrum based watermark verification algorithm with the seed X, the stego data SD, and the resulting payload Y).

TVP

Time variant parameter, such as a sequence number or a time stamp.

RPMG(X,Y)

A random phase mask generator, where X denotes the cryptographic key as input data and Y denotes the resulting phase mask as output data.

DIES(PM,OI,CD)

A symmetric digital image encryption scheme, which is based on the Fourier transform of the image, phase modification (random mask encoding by multiplication on the complex exponential component $e^{j\varphi(m,n)}$), inverse Fourier transform, and quantization, where PM denotes the phase mask and ID denotes the original image as input data and OI denotes the ciphered image as output data.

FFTS(CO, S_R, SMC)

A component selector function of the real and imaginary FFT components. CO denotes the cover image, S_R the applied selection rule function, and SMC the resulting set of FFT magnitude components.

AF(SMC, HF, MS)

An authentication function of the selected FFT magnitude components, where SMC denotes the identified magnitude components, HF denotes the applied crh, and MS the resulting authentication message as a string of arbitrary length. For example, AF(SMC, HF, MS) consists of generating a string from each selected Fourier component, concatenating these strings and applying a hash function to the resulting string.

K_{XY}

A secret key for a symmetric cryptosystem shared between two entities with the distinguished name X and Y.

K_{XY}[Data]

denotes the cipher text generated by a symmetric cryptosystem with plain text Data.

||

Concatenation of two data elements.

CD

Cover Data

SD

Stego Data

II. Copyright/Content/Originality protection based on a spread spectrum technique

Depending on the proof-level to be provided for the protection, the preferred embodiment of the apparatus and method according to the invention provides three different levels of reliability, which are based on each other, namely: individual copyright/content/origin-

ality protection, copyright/content/originality protection with registered cryptographic keys, and copyright/content/originality protection with an CCC on the basis of registered cryptographic keys.

Due to commercial requirements, the system provides different protection aspects, nameley content protection, copyright protection, and originality verification of the stego data.

The copyright protection of a multimedia data set is considered as the process of proving the intellectual property rights to a court of law against unauthorized reproduction, processing, transformation, or broadcasting on the basis of digital evidence data. This process is based on a watermarking process WP and a registration process RP. RP is executed after WP has been initiated and finished. RP is executed by a third party, which represents a different legal entity as the Copyright Holder (CH), and provides digital evidence data for the CH required for verifying copyright ownership. The specific cover- or stego data is a digital image, or video data. The WP embeds or extracts owner authentication data in or from multimedia data sets. This owner authentication data is embedded such that the commercial usability of the multimedia data set is not affected. For this purpose, a key is applied to embed encoded owner authentication data, called the watermark, into the cover data set I, resulting in a stego data set I*. The watermark data can then be extracted from the stego data if the correct key is used.

In the following, WP is based on a perceptually adaptive spread spectrum technique, a specific type of a symmetric cryptographic system. In order to embed or extract a watermark, it is necessary to know the exact values of the seed used for the generation of pseudo random sequences used to encode the watermark. Because spread spectrum signals are statistically independent (and therefore virtually orthogonal), more than one wa-

termark may be encoded into the multimedia data set. Depending on the seed applied for the embedding and verification, we distinguish between a private and a detection watermark. A private watermark is defined as encoded owner authentication data embedded with a cryptographic signature as the seed. A detection watermark is defined as encoded owner authentication data embedded with a cryptographic secret key as the seed. We differentiate between copyright protection, content protection, and originality protection.

Originality protection is considered as a process applied after the copyright protection process. It enables a third party to check if the image contents has been modified on the basis of a public watermark.

Content protection is considered as an additional process applied during the trading transaction between a service provider and a customer. The content protection described is based on the transform domain of the image data and not on cryptographic ciphering algorithms applied during the communication between the service provider and the customer, since these cryptographic algorithms are not robust against loosely compression and other image transformations. In addition, the performance of ciphering algorithms for the content protection of image or video data is very time consuming.

The present method and apparatus is based on an image or video watermark technique, described below, which embeds and detects the the payload of a Watermark. This technique is based on a perceptually adaptive spread spectrum technique which provides reliable means of embedding robust watermarks. Such a technique will be discussed in section III. In addition, a spread spectrum techniques is a form of symmetric cryptosystem. In order to embed or extract a watermark, it is necessary to know the exact values of the seed used to produce pseudo random sequences used to encode a watermark. The seeds are

considered to be cryptographic keys for watermark generation and verification. System security can therefore be based on proprietary knowledge of the keys and provide in addition the necessary security parameters needed for a secure communication (mutual authentication, integrity, confidentiality, non-repudiation) in the trading process of digital images or videos. Because spread spectrum signals are statistically independent (and therefore virtually orthogonal), the present method and apparatus encodes more than one watermark in an image or video frame at the same time, namely detection, private watermarks and public watermarks. The detection watermark allows to identify during a scanning process if the stego data belongs to the copyright material of a CH. The generation of the private watermark is based on a digital signature as the seed and supports, therefore, third party verification who has generated the seed information for the coding and the decoding of the payload. The generation of the public watermarks enable the verification of the originality of the received stego data on the private key of the asymmetric key pair of the ICH.

Since the system provides for the registration of the public key of the asymmetric key pair, the CH can prove that he is the only person in the possession of the adequate private key of the asymmetric key pair and, therefore, the generator of the private watermarks.

The system also provides the secure registration (mutual authentication, integrity, non-repudiation) of watermark encoded images (stego data sets) at a CCC. The stego-image is registered at the CCC and a digital copyright certificate is generated which is signed by the CCC. If an unauthorized third party has also encoded watermarks in the same image, conflicting claims in copyright disputes can be resolved. Examining the time stamps of the copyright certificate enables the secure identification of the legal owner: The earliest of the time

stamps identifies the legal owner if no copyright revocation request has been applied.

Watermark protection with registered cryptographic keys and the CCC based copyright protection are based on a PKI. The PKI issues on request public key certificates containing the public key of the party, the distinguished name of the party, and a time stamp. Every certificate is signed with the PKI's private key and the trust is built on the validity of the authentic copy of the PKI's public key (we assume that the public key of the PKI is accessible, authentically distributed, and verifiable by every party).

In the following three levels of the system are described.

The method described in this section II requires a suitable watermarking technique. Various such techniques are known and can be employed. However, a preferred technique is described in the section III.

II a) Registration based copyright, content, and originality protection

Depending on the proof-level to be provided for the protection, our approach provides three different protection levels, which are based on each other, namely individual copyright/content/originality protection, copyright/content/originality protection with registered cryptographic keys, and copyright/content/originality protection with a CCC on the basis of registered cryptographic keys. Since the first two cases are special cases of the third one, we present only the approach for the registration based copyright protection. Depending on the level of protection to be provided (content or originality or copyright protection), not all phases described below have to be executed. The phases described below have to be executed for the highest level of protection, i.e. content and originality and copyright protection. Based on one asymmetric key pair only, H can enforce the

different protection mechanisms for copyright, originality, and content protection.

As shown in Fig. 3, the system for the CCC based protection is partitioned into four processes, namely the CH with the name H, the B process with the name B, the PKI process with the name I, and the CCC process with the name C. Suppose (ps_H, vs_H), (pc_H, vc_H), (ps_B, vs_B), (pc_B, vc_B), (ps_I, vs_I), (pc_I, vc_I), (ps_C, vs_C), and (pc_C, vc_C) are the asymmetric key pairs of H, B, I and C, respectively and all the involved parties would like to exchange information by on-line communication. (In the case of off-line communication, the security mechanisms to be provided for the communication are covered by operational means). H has an authentic copy of $Cert_B$ and $Cert_C$ whose signatures were verified with the authentic copy of vs_I. B has an authentic copy of $Cert_H$ and $Cert_C$ whose signatures were verified with the authentic copy of vs_I. C has an authentic copy of $Cert_H$ and $Cert_B$ whose signatures were verified with the authentic copy of vs_I. The following phases are then applied:

Phase 1:

H retrieves the cover data CD, generates a unique identifier $ID_{CD} := crh(H||SN)$, where SN is a serial number, stores ID_{CD}, and retrieves the key pair (ps_H, vs_H).

Phase 2:

Detection watermark embedding (image owner authentication and copyright protection)

H generates the stego data SD applying the transformation: $OWEA(crh(ps_H), SN||SN, CD, SD)$.

Phase 3:

Private watermark embedding (copyright protection)

1. H generates the private Owner Authentication Data OAD_{CD} applying $DSSMR_G(ps_H, ID_{CD}, OAD_{CD})$.
2. H generates the stego data SD applying the transformation: $OWEA(crh(OAD_{CD}), ID_{CD}, CD, SD)$, where CD is the SD of the last phase.

Phase 4:

Public watermark embedding (originality protection)

1. H generates the set of magnitude components, applying FFTS(CD, S, MC), with the selection function S and the resulting set MC of the FFT magnitude components. S is given by the normalization of the magnitude components with the JPEG or MPEG quantization table entries and constrained by these components that will be modified during the coding process of the public watermark.
2. H then generates the authentication data for originality verification, applying AF(MC, crh, AM), where MC denotes the in the last step generated FFT magnitude component set, crh the applied hashing function, and AM the resulting authentication message as output. AM is generated by converting the value of every magnitude component into a string and concatenating the resulting strings of every magnitude component into one string.
3. AM is then ciphered with the key pc_H, i.e. pc_H[AM] and embedded as the payload in the public watermark, applying OWEA(crh(vs_H), pc_H[AM], CD, SD), where CD is the SD of the last phase.

Phase 5:

H then stores the resulting stego data SD.

Phase 6:

H and C execute the following steps for the secure registration or validation of copyright requests, and the generation of copyright certificates.

1. H generates first the copyright request data CRD, CRD := crh(SD||SN) and then the copyright request CR, CR := <TD||SigTD>, with TD := CRD||TVP||H||C, and $DSSAP_G$(ps_H, TD, SigTD). H then transmits CR to C.
2. C receives CR and verifies TD, applying $DSSAP_V$ (vs_H, SigTD, IVR), where IVR denotes the intermediate verification result. If IVR = crh(TD), with TD := CRD||TVP||H||C, then TD has been successfully veri-

fied and the next step shall be executed. In any other case, the processing and communication between the H and C is stopped.

3. If verification was successful, C generates the corresponding digital copyright certificate executing $DSSAP_G(ps_C, CCD, SigCCD)$, with CCD:= CRD||TVP. C then stores the copyright certificate CC := CCD||SigCC and generates then the Copyright Confirmation Reply CCR, CCR := <TD||SigTD>, with TD := CC||TVP||C||H, and $DSSAP_G(ps_C, TD, SigTD)$. C then transmits CCR to H.

4. H receives CCR and verifies TD, applying $DSSAP_V(vs_H, SigTD, IVR)$, where IVR denotes the intermediate verification result. If IVR = crh(TD), with TD := CC||TVP||C||H, then TD has been successfully verified. H then verifies and stores the CC. The following phase can now be executed repeatedly, if necessary, without repetition of the previous phases.

Phase 7:

H and B execute the following steps for the trading of copyright, content, and originality protected digital data (images and video):

1. B generates the trading transaction T1, T1 := <TD||SigTD>, with TD := ID_{CD}||TVP||B||H, and $DSSAP_G(ps_B, TD, SigTD)$. B then transmits T1 to H.

2. H receives T1, verifies TD, applying $DSSAP_V(vs_B, SigTD, IVR)$ where IVR denotes the intermediate verification result. If IVR = crh(TD), with D := ID_{CD}||TVP||B||H, then TD has been successfully verified and the next step shall be executed. In any other case, the processing and communication between the H and B is stopped.

3. If the verification was successful, H retrieves with the ID_{CD} information the corresponding stego data SD and generates the trading transaction T2 := <TD||SigTD>, with TD := CD||TVP||H||B, DIES(PM, SD, CD) with $RPMG(DSSMR_G(ps_H, B||SN), PM)$, and $DSSAP_G(ps_H$,

TD. SigTD). B||SN designates the B and the picture and is called the mask message. H then stores $DSSMR_G(ps_H, B||SN)$ and transmits T2 to B.

Phase 8:

B receives T2 and verifies TD, applying $DSSAP_V(vs_H, SigTD, IVR)$, where IVR denotes the intermediate verification result. If IVR = crh(TD), with TD := CD||TVP||H||B, then TD has been successfully verified and CD is locally stored.

Phase 9:

After B has paid, H retrieves IK_B and sends $vc_B[IK_B]$. B receives $vc_B[IK_B]$, deciphers it ($pc_B[vc_B[IK_B]]$), and generates the random phase mask PM. This random phase mask is then used for deciphering CD (DIES(PM, CD, SD)) to get the original stego data SD.

Phase 10:

B may verify the originality of the stego data SD, retrieving the public key from H and applying $OWVA(crh(vs_H), SD, pc_H[AM])$. B then deciphers $pc_H[AM]$ applying $vc_H[pc_H[AM]]$. H then verifies AM applying the same steps 1 and 2 as described in phase 4. If the verification was successful, the image content has not been altered. If the watermark has been destroyed or overwritten, the contents of the SD has been modified. If the verification fails, the content has also been modified by unauthorized parties.

Remark:

Depending on the applied asymmetric scheme the private decipherment key may be identical to the private signature key and the public encipherment key may be identical with the public verification key.

Since the generated asymmetric key pairs are unique, the CH can be uniquely identified on the basis of the digital copyright certificate.

B may check the copyright certificate requesting C (or H) to transfer an authentic copy of the copyright certificate for a given identifier ID_{CD}. Except

the data transferred, the applied protocol is the same as described above (see phase 6).

If H would like to transfer a specific copyright of a CD set to another legal party, he may initiate a copyright revocation request with C. The different phases of this request are analogue to the copyright request.

For copyright verification, the CH first verifies the detection watermark and then the private watermark with the extracted SN.

Copyright verification may be checked by a third party, if the H transfers the digital signature applied for the seed. Based on the retrived bublic key from H, the third party can verify that H is the only one who has generated the corresponding signature.

II.b) Copyright, content, and originality protection with registered keys

As shown in Fig. 2, the apparatus for the copyright, content, and originality protection with registered cryptographic keys is partitioned into three processes, namely the CH with the name H, the Buyer process with the name B, and the PKI process with the name I. Suppose (ps_H, vs_H), (pc_H, vc_H), (ps_B, vs_B), (pc_B, vc_B), (ps_I, vs_I), and (pc_I, vc_I) are asymmetric key pairs of H, B, and I, respectively. Suppose H has an authentic and actual copy of $Cert_B$ which signature was verified with the authentic copy of vs_I and the B has an authentic and actual copy of $Cert_H$ which signature was verified with the authentic copy of vs_I. Then the same phases except phase 6 as for II.a) have to be applied.

Remark:

Since the generated asymmetric key pairs are unique, the CH can be uniquely identified if no additional watermarks by unauthorized persons have been encoded into the SD.

II.c) Individual copyright, content, and originality protection

As shown in Fig. 1, the apparatus for the individual copyright , content, and originality protection is partitioned into two processes, namely the CH with the distinguished name H and the B process with the distinguished name B. Suppose (ps_H, vs_H) and (pc_H, vc_H) are asymmetric key pairs of H, (ps_B, vs_B) and (pc_B, vc_B) are the asymmetric key pairs of B. Suppose H has an authentic copy of vs_B, vc_B and B has an authentic copy of vs_H, vc_H. Then the same phases as for II.b) have to be applied.

Remark:

In the case of a legal copyright dispute, H can retrieve the payload of the detection watermark and construct the signature taken as the seed for the private watermark. Since the generation of the same asymmetric key pair by two distinguished entities is very unlikely, the generation of the digital signature as the seed for the private watermark provides a good level of proof against copyright infringement. In the case of watermark protection with registered keys, the generation of the same asymmetric key pair by two distinguished entities can be prevented.

III. Embedding the watermarks

The watermarking technique described here comprises the following steps:

a) An error-control coding technique for the message to be transmitted in the watermark;

b) A method to encode respectively to decode the message resulting from step a);

c) A reliable method for embedding the encoded message from step b) in the image or video without introducing visible artifacts.

d) A watermark extraction technique that is robust against compression, translation, rotation, scaling or change of proportion of the stego image or video.

e) A watermarking technique for small and or irregular blocks.

f) A method that allows to detect if a stego-image was marked or not with a given key without extracting the encoded message.

g) A method for watermarking without template which is resistant to translation, rotation and scaling.

h) A method for watermarking videos.

Each of these aspects can be applied to conventional watermarking techniques. Preferably, they are used in combination to provide a highly reliable, robust and powerful method for marking data sets. This method can be applied for any watermarking applications, in particular to the application described in section II of this disclosure.

Steps a) and b) can be used for embedding watermarks in any type of data while steps c) is optimized for embedding watermarks in images or video frames.

In the following, the above mentioned elements of the watermarking technique are described in detail.

III.a) Error control coding

Error control coding is applied to the message prior to encoding step III.b). When used in combination with the procedure described in section II, the message corresponds to one of the blocks BL_i.

Preferably, symbol based Reed Solomon (RS) codes are applied for this purpose. The advantages are the following:

- RS codes correct symbol errors rather than bit errors, and

- RS codes can correct erasures as well as errors. Erasures can be factored out of the key equation, which means that "erased" symbols can be ignored. They do not play any role in the error control mechanism - an erasure is useless redundancy.

Being able to discard erased symbols has two advantages:

- If the posterior probability of a received symbol is low, it may be ignored.

- RS codes only come in standard sizes. For example a 255 x 8 bit code is common. Most commonly used RS error control codes appear to be too large to be used in watermarking. However, it is possible to make almost any RS code fit a watermarking application by judiciously selecting symbols as being erased (because they were never embedded in the image in the first place).

III.b) Encoding the message

During encoding, the message to be transmitted in the watermark is transformed into a form suited for being used in the modulation of image components. At the same time, it is encrypted using a suitable key.

If used with the method of section II, the encoding procedure has access to the cryptographic keys p_H and v_H (or their hash values), which are applied as seeds to generate pseudo-random sequences as described below. The public key is used for encoding the message of the public watermark, the private key is used for the private watermark. Knowledge of the corresponding key (or hash value) is required for recovering the message from the watermark.

A watermark may be embedded or extracted by the key owner. In this form spread spectrum is a symmetric key cryptosystem. From the point of view of embedding watermarks in images or videos given the cryptographic keys the sequences themselves can be generated. A good

spread spectrum sequence is one which combines desirable statistical properties such as uniformly low cross correlation with cryptographic security.

Suppose we are given a message B (e.g. that was provided with error coding in above step III.a). The message has the binary form $b_1b_2...b_L$, where b_i are its bits. This can be written in the form of a set of symbols $s_1s_2 . . . s_M$ - most generally by a change in a number base from 2 to B. The next stage is to encode each symbol s_i in the form of a pseudo random vector of length N, wherein each element of this vector either takes the value 0 or 1. N is e.g. in the order of 1000 to 20000 (in the order of 10%-50% of the total number of image coefficients (Fourier components) that can, theoretically, be modulated).

In a preferred embodiment, this is carried out by using a pseudo random generator seeded by the key $crh(p_H)$ or $crh(v_H)$.

To encode the first symbol a pseudo random sequence v of length N + B - 1 is generated. To encode a symbol of values where $0 \leq s < B$ the elements v_s, v_{s+1} ... v_{s+N-1} are extracted as a vector $\mathbf{r}_1$ of length N. For the next symbol another independent pseudo random sequence is generated and the symbol encoded as a random vector $\mathbf{r}_2$. Each successive symbol is encoded in the same way. Note that even if the same symbol occurs in different positions in the sequence, no collision is possible because the random sequences used to encode them are different - in fact they are statistically independent. Finally the entire sequence of symbols is encoded as the summation:

$$\mathbf{m} = \Sigma_{i=1..M} \mathbf{r}_i$$

The pseudo-random vector $\mathbf{m}$ has N elements, each varying between 0 and M. In a next step, the elements of $\mathbf{m}$ are offset to make their mean zero. These elements will determine the strength of modulation of the Fourier components of the image in step III.c.

When decoding the watermark, a vector **m'** (read-out message) is derived from the stego-image. In oblivious watermarking, **m'** corresponds to the modulated Fourier coefficients. Hence, in general **m'** will not be equal but "similar" to **m**.

To decode s from **m'**, the elements of **m'** are first offset to make their mean zero. Then, starting from the (known) seed, the first random sequence v of length N + B - 1 is generated and the correlation of v with **m'** is calculated. The peak of the correlation indicates the offset s_1 in the random sequence that was used for generating $\mathbf{r}_1$. Then, the next random sequence v is generated and cross-correlated with **m'** to retrieve s_2, etc.

Reliable communications of the apparatus are best accommodated by using m-sequences or Gold Codes to generate the random sequences $\mathbf{r}_i$ and use amplitude modulation:

$$\mathbf{m} = \Sigma_{i=1..M}\ \mathbf{b}_i^*\ \mathbf{r}_i^*$$

where $\mathbf{b}_i^*$ and $\mathbf{r}_i^*$ are $\mathbf{b}_i$ and $\mathbf{r}_i$ in which each bit 0 was replaced by 1 and each bit 1 by -1 due to the isomorphism between the group (exclusive OR, (0,1)) and (*, (1,-1)). In this case the values of **m** are between -M and M. Then the decoding is carried out by simply cross correlating with each of the random sequences $\mathbf{r}_i$ in turn. If the correlation is negative then a binary one has been sent, otherwise a binary 0.

Gold codes and m-sequences, both insure a good reliability and security of the embedded mark. However, Gold codes have the advantage that for a given register length k ($N=2^k-1$) there is a larger choice for the key ($2^{2k}-1$ instead of 2^k-1) and a better correlation properties if only part of the sequence is used.
If M is sufficiently large, the statistical distribution of the message **m** should approach a Gaussian (Central Limit Theorem). A Gaussian distributed watermark has the advantage that it is more difficult to detect. The vari-

ance increases with order $M^{1/2}$; in other words, the expected peak excursion of the sequence is only order $M^{1/2}$.

III.c) Embedding the message in the image or video

In this step, the encoded message **m** (e.g. as obtained in the previous step) is applied to the image or a video for generating the watermark.

In contrast to steps III.a) and III.b), embedding the message in the image requires some knowledge of the nature of the data stored in the image. In the following, the image is assumed to be a two-dimensional image that can be a still image or a video frame. The method is optimized for robustness against operations generally applied to images or video frames such as translation, cropping, rotating, scaling, change of proportion. (The method is not optimized for other types of data, such as sound or text.)

In order to achieve robustness against circular translation, the image block is first subjected to a Fourier transform. Then, message **m** is used to modulate the Fourier components. In addition to this, a template is embedded in the image, which template can be used for detecting rotation, scaling or change of proportion of the image when reading the watermark. A tiling mechanism and suitable phase-dependent correction are applied for providing robustness against cropping.

Figure 4 shows a detailed diagram describing the embedding of the watermark. Calculation starts from the cover image:

1. If the image is a color image, then compute the luminance component (by replacing each pixel by $g/2 + r/3 + b/6$, where g, r and b are its green, red and blue components) and use these values for the following calculations.
2. If a predefined block size (N_b) is used, divide the image into adjacent blocks of size N_b x N_b (e.g. 128 x

128 pixels). Otherwise N_b is the minimum of the image height and width (N_b =min(height, width)).

3. Map the image luminance levels (or gray levels for a black and white image) because it corresponds to a perceptually "flat" domain by replacing them with their logarithm. The logarithm is a good choice because it corresponds of the Weber-Fechner law which describes the response of the human visual system to changes of luminance.
4. Compute the FFT (Fast Fourier Transform) of each block. From the real and imaginary components obtained in this way, calculate corresponding magnitude and phase components.

   The magnitude components are translation invariant and will therefore be used in the following modulation steps. (However, it is possible to derive translation invariants from the phase spectrum as well, which could also be modulated).
5. Select the magnitude components to be modulated. To encode a message **m** of length N, a total number of N components are modulated. In non-oblivious watermarking, any components can be modulated. For oblivious watermarking, because of interference of the cover image with the watermark, the largest (highest energy) components (at about the lowest 10% of the frequencies) are avoided and components at medium frequencies (about next 30%-50%) are used; these frequencies are adjacent and are thus located in a band of frequencies. These figures are chosen because they generally give a good compromise between robustness and visibility of the watermark.

   There are several methods for selecting the components to be modulated, for example:

   a) The selection of the components to be modulated does not depend on the given image. Rather, the same components are selected for every image. The author as well as the reader of the watermark know

either the positions of the components to be selected in advance or a key which allows by means of a pseudo-random generator seeded by this key to generate the positions.

b) The largest components (inside the allowable frequency range) are used for modulation.

c) Almost all magnitude components in a given frequency band are used. The upper limit of the band is computed such that the number of frequencies inside the band be larger than and as close as possible to N.

In the methods b) and c) the order in which the components to be modulated can be provided by a pseudo-random generator seeded by a key known by both, author and reader.

When selecting the components to be modulated, care must be taken to preserve the symmetry imposed on the Fourier components $F(k_1, k_2)$ by the fact that the image block is real valued:

$$F(k_1, k_2) = F^*(N_b - k_1, N_b - k_2)$$

Once the magnitude components $(M_1, \ldots M_N)$ to be modulated are chosen, the corresponding value m_i of message **m** is added to or subtracted from the corresponding selected magnitude component M_i. Addition is used, if the corresponding phase component P_i is between 0 and π, subtraction if it is between π and 2π. This provides robustness against translation and cropping (see below).

Before adding/subtracting the values m_i to/from M_i, the vector **m** can be scaled to adjust the magnitude of its elements to those of the components M_i. Generally, the elements m_i should be of the same order of magnitude as the components M_i. The depth of modulation or amplitude of the embedded signal should depend on the objective measure of the perceptual significance. The lower the perceptual significance, the higher should be the amplitude of the watermark.

Moreover, to insure a good invisibility one can use local energy and masking criterion (see J.F. Delaigle, C. De Vleeschouwer, B. Macq, "Digital watermarking", Proceedings of the SPIE Electronic Imaging Science and Technology, vol. 2659: Optical Security and counterfeit Deterrence Techniques, San Jose, February 1996) to determine the depth of modulation. However, for simplicity, the amplitude for all components is kept constant. This constant can be predefined by the owner or can be some function of the mean and/or the variance of the energy in the image or its Fourier transform and the values of the pseudo-random vector **m** containing the encoded message (e.g. (mean(energy) + a * variance(energy))/mean(**m**), where a is a predefined constant).

6. Add a template by a second modulation of the magnitude components. This is described in more detail below.
7. Compute the inverse FFT using the phase components and the modulated magnitude components.
8. Compute the inverse of the perceptual mapping function of step 3. For Weber-Fechner law mapping, the inverse function is an exponential.
9. Replace each watermarked block in the image to obtain the stego-image.
10. If the image is a color image, then rescale the red, green and blue components by the relative change in luminance introduced by embedding a watermark. Typically, the red, green and blue pixels occupy a byte each in program memory. If overflow or underflow occurs then the pixel is set to the upper bound 255 or lower bound 0 respectively.

<u>Template</u>

As mentioned above, a template is added to the image in step 6. Two kinds of templates can be used:

a) a RST template – to detect rotations and scaling

b) a PST template - to detect horizontal and vertical scaling.

The PST template is rather used in case of video frames (changes of proportion are more likely to occur in the case of videos than rotations) and the RST is rather used for still images (photographs, paintings, etc. . .).
The steps for generating the template are illustrated in Fig. 5:

20. Apply a log-polar or a log-log map to the magnitude components. The log-polar map transforms the magnitude components of the FFT into a polar coordinate system (Θ, log-r) with logarithmic radius axis as follows. Consider a point $(x,y)\in\Re^2$ and define:

$$x = e^{\mu} \cos \Theta$$
$$y = e^{\mu} \sin \Theta$$

where $\mu\in\Re$ and $0 \leq \Theta < 2\pi$. If $r = e^{\mu}$, $\mu = \log(r)$ and for every point(x,y) there is a unique $(\Theta, \log(r))$ that corresponds to it. In the log-polar representation, a scaling of the image leads to an offset of the components along the log-r axis and a rotation of the image leads to an offset along the Θ axis. Similarly, the log-log map transforms the magnitude components into a logarithmic coordinate system (log-x, log-y) as follows. For each point $(x,y)\in\Re^2$ define:

$$x = e^{\alpha}$$
$$y = e^{\beta}$$

Then, $\alpha=\log(x)$ and $\beta=\log(y)$, and in this log-log representation, the horizontal respectively vertical scaling leads to offsets along the log-x respectively log-y axes.

21. Preferably, low pass filtering is used for interpolating the frequency space components during this mapping. The magnitude components belonging to very low or high frequencies are not mapped. The following modulation is only applied to components in medium frequency range.

22. Select the magnitude components in the log-polar or log-log coordinate system to be modulated. Typically, about 0.1-0.3% of all components are to be modulated. The RST or PST pattern **T** formed by the selected components in log-polar or log-log space should be such that its auto-correlation under translation is weak. For this purpose, the indices of the selected components should be coprime or be derived from a two-dimensional random sequence. This random sequence can be generated by a random generator seeded by a key K. Whoever knows this key K will be able to reconstruct the template and detect the watermark as explained below. Each selected component is increased by a given value.
23. Map the modulated points by change of coordinates back into frequency space (inverse log-polar mapping or inverse log-log mapping).

The RST or PST pattern **T** formed by the selected components in log-polar respectively log-log space is predefined and known to the reader of the watermark.
It must be noted that the calculation of the log-polar respectively log-log transform of the cover image or video frame is not required for generating the template. Instead, the RST or PST pattern **T** of the components to be modulated in log-polar respectively log-log space can be mapped back to frequency space, which results in a RST or PST pattern **T'** in frequency space that can be applied directly to (e.g. added to) the components in frequency space. Alternatively, the template can be added directly in the Fourier transform domain.
As will be explained below, the template is not required for non-oblivious watermarking.

III.d) Extracting the watermark from the stego-image or video

Figure 6 shows a detailed diagram illustrating the steps for reading a watermark from the stego-image or stego video frame:

31. If the image is a color image then compute the luminance component and use these values for the following calculations.
32. If predefined block size (N_b) is used, divide the image into adjacent blocks of size N_b x N_b (e.g. 128 x 128 pixels). Otherwise N_b = min(height, width).
33. Map the image luminance levels (or gray levels) to the perceptually "flat" domain by replacing them with their logarithm.
34. For each block compute the FFT.
35. Use a data windowing process to suppress the edge effects in the magnitude spectrum due to possible rotation or scaling of the image. Different windows can be used such as Blackman, Hamming, Hanning, Welch or Bartlett Window (see W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery, "Numerical Recipes in C", Cambridge University Press, second edition, 1992). The effect of data windowing in the space domain is equivalent to convolution in the frequency domain with a narrow filter. The blurring effect introduced by this convolution is beneficial because it tends to smooth the spectrum which makes interpolation more effective.
36. Determine the rotation and scaling that the image suffered by finding the RST template in log-polar space or determine the horizontal and vertical scaling by finding the PST template in the log-log space. These steps are described below in "Finding the template" section.
37. Using the results of step 35, read the modulated components to generate message **m'**. This requires the knowledge of the method that was used in step 5 for selecting the components to be modulated.

Once that the message **m'** is recovered, it is demodulated and error corrected using the methods described in sections III.a) and III.b).

<u>Finding the template</u>:

The steps for finding the template are illustrated in Fig. 7:

40. Apply log-polar or log-log mapping to the magnitude components of the Fourier transform. The magnitude components belonging to very low or high frequencies are not mapped. The following analysis is only applied to components in medium frequency range or to all components except the low frequency range.

41. For oblivious watermarking, calculate the normalized cross correlation of the components in log-polar or log-log space with the RST or PST pattern **T** that was used for generating the template in step 21 and find the point of best correlation. If the image has neither been rotated or scaled, this point is at zero. If the image is rotated and/or globally scaled there is an offset along the Θ axis and/or log-r axis in the log-polar map. If the scaling suffered by the image or video frame was different on horizontal respectively vertical axis, there are offsets along log-x respectively log-y axes in the log-log map. For non-oblivious watermarking, the log-polar respectively log-log transform of the Fourier components of the cover image can be used instead of RST or PST pattern **T** for retrieving scaling, rotation respectively change of proportion. The cross correlation can be calculated efficiently using conventional Fourier techniques.

In order to obtain better results and lower computational cost, before applying the cross correlation one can first adaptively filter the data to remove outliers and noise and use a filter which keeps only local peaks. This can e.g. be carried out by locally calculat-

ing the variance (or some other value indicative of the data's distribution) of neighbouring data of each data point. If a given data point lies clearly outside this variance, is it replaced by zero. In a next step, local peaks that have not been filtered out are then stored in a sparse matrix to reduce computation. The fast correlation (using the FFT or by a point by point correlation) is done in this case between the peaks of (**T**) and the peaks of (**T'**). The correlation can moreover be weighted so that the more reliable central points are more strongly weighted.

It is possible to further increase accuracy of the scaling and rotation factors by carrying out the following: detecting a scaling and/or rotation in a first iteration from the correlation between the log-polar or log-log transform and the template, using said scaling and/or rotation for either a) scaling and/or or rotating said Fourier transform, calculating a scaled and/or rotated log-log or log-polar transform therefrom and correlating said rotated log-log or log-polar transform with said template, or b) calculating a second template by scaling and/or rotating an original Fourier-space template and calculating a log-log and or log-polar transform therefrom and using said second template for calculation a second correlation with said log-log or log-polar transform of said stego data

III.e) Embedding watermarks in small and/or irregular blocks

To embed watermark in small blocks, one computes the transform over regions that instead of comprising only one block, extend over adjacent blocks. To do this one can use the Lapped Orthogonal Transform (see H.S. Malvar, "Signal Processing with Lapped Transforms", Norwood, MA, 1991), which has the advantage to minimize blocking effects which would otherwise make a strong watermark based

on blocks visible, especially for small block sizes. This is followed by the method as described in III.c and III.d, where the Fourier transformation phase is replaced by the Lapped Orthogonal Transform (LOT) application for the cover image, while keeping the same template operations.

Using small blocks (of roughly 16 by 16 points) allows the strength of the embedded message to be modulated as a function of the local variance, which renders the method adaptive. Furthermore the watermark can be recovered locally the only requirement being that a sufficient number of blocks are available to contain 1 complete message. To embed watermark in blocks with irregular shapes (non-square and non-rectangular) such as might occur in MPEG4 video compression, two possible solutions can be applied:

- padding of the irregular blocks in order to obtain square blocks, using either constant padding, or symmetrical padding, then method as in III.c and III.d;
- avoid the padding phase by directly using wavelet transforms of arbitrary length signals (see H.S. Barnard, Image and Video Coding Using wavelet decomposition, CIP-Gegevens, Koninklijke Bibliotheek, Den Haag, 1994). This is followed by the method as described in III.c and III.d, where the Fourier transformation phase is replaced by the Wavelet Transformation for the cover image, while keeping the same template operations.

III.f) Watermark detection without extraction

Being able to detect a watermark without being able to decode it is useful and in many cases sufficient to prove the identity of the generator of the watermark. This can be done by a Bayesian approach (see J.J.K. Ó Ruanaidh and W.J. Fitzgerald, "Numerical Bayesian Methods Applied to Signal Processing", Series on Statistics and

Computing, Springer-Verlag, 1996) that allows to compute the probability that a watermark generated by a given key is present in the stego-image, relatively to the probability that no watermark was generated with that key.

The implementation of this principle operates as follows. The used watermark **d** is a linear combination of pseudo-random sequences corrupted by noise:

$$\mathbf{d} = \mathbf{G}\,\mathbf{b} + \mathbf{e}$$

where **e** is a noise vector corrupting the watermark, **b** is an M x 1 vector and **G** is an N x M matrix of bits in form +1 and -1 (due to the isomorphism between the group (exclusive OR, {0,1}) and (*, {1,-1}) 0 was changed to 1 and 1 to -1). Each column of **G** is a pseudo-random sequence such as an m-sequences or a Gold Code in which 0 was changed to 1 and 1 to -1.

If we assume that the noise follows a Gaussian distribution, the probability that a message of length M was embedded with a said key k in the stego-image (SD) is:

$$p(k, \mathrm{M} \mid \mathbf{d}, SI) \propto \frac{\pi^{-\mathrm{N}/2}\Gamma(\mathrm{M}/2)\Gamma((\mathrm{N}-\mathrm{M})/2)\det(\mathbf{G}^{\mathrm{T}}\mathbf{G})^{-1/2}}{4R_\delta R_\sigma(\hat{\mathbf{b}}^{\mathrm{T}}\hat{\mathbf{b}})^{\mathrm{M}/2}(\mathbf{d}^{\mathrm{T}}\mathbf{d}-\mathbf{f}^{\mathrm{T}}\mathbf{f})^{(\mathrm{N}-\mathrm{M})/2}}$$

where Γ is the gamma function, R_δ and R_σ are irrelevant constants introduced as normalization factors,

$$\hat{\mathbf{b}} = (\mathbf{G}^{\mathrm{T}}\mathbf{G})^{-1}\mathbf{G}^{\mathrm{T}}\mathbf{d}$$

and

$$\mathbf{f} = \mathbf{G}^{\mathrm{T}}\hat{\mathbf{b}}$$

The probability that no message was embedded with the said key k in the stego-image (SD) is:

$$p(k, 0 \mid \mathbf{d}, SI) \propto \frac{\pi^{-\mathrm{N}/2}\Gamma(\mathrm{N}/2)}{2R_\sigma\;(\mathbf{d}^{\mathrm{T}}\mathbf{d})^{\mathrm{N}/2}}$$

Finally, we compute the relative log-probability:

$$\log\left(\frac{p(k,\mathrm{M}\mid\mathbf{d},SI)}{p(k,0\mid\mathbf{d},SI)}\right)$$

and compare with 0.

III.g) Watermarking without template

Using a combination of Fourier transform and a log-polar map, i.e. the Fourier-Mellin transform that is the Fourier transform of a log-polar map, allows to embed a watermark in a domain that is invariant to rotation, scale and translation, without the need to use a template to detect rotations and scaling. The method consists of directly transforming the cover-image or -video frame in the log-polar domain; the watermark is directly inserted at this stage. Figure 8. shows the steps for embedding the watermark in a rotation, scale and translation invariant domain.

An alternative which is computationally more efficient bypasses the mapping of the original image or video frame in the rotation, scale and translation invariant domain. This is shown in Figure 9. The scheme to extract the watermark from the image is shown in Figure 10.

Replacing the log-polar mapping by the log-log mapping allows to embed a watermark in a domain that is invariant to translation, horizontal and vertical scaling.

This is an idealized watermarking scheme which works in principle but which in practice is quite costly and difficult to implement. The first difficulty is that both the log-polar mapping (LPM) and the inverse log-polar mapping (ILPM) can cause a loss of image quality. The change of coordinate system means that some form of interpolation must be used. This leads to a second difficulty, which is rather numerical. Interpolation only performs well if the neighboring samples are of the same

scale, which is not verified by the magnitudes of the frequency components.

III.h) Watermarking videos

In the case of uncompressed video each frame is marked. One possibility is to use the same key and the same watermark in each frame. However this can decrease the robustness of the watermark against forgery. Therefore, it is preferable to use the same key, but a different watermark for each frame (e.g. the label of the video followed by the frame number). In the case of MPEG1 or MPEG2 compressed video, only the intraframes I (the first frame of each group of pictures) are marked.

Another novel alternative for watermarking uncompressed video is to individually mark three-dimensional spatio temporal blocks of video stream, which may be overlapped in time and/or in space. The method used here is an extension of the algorithms used for 2D images to the temporal dimension, using 3D Fourier transform, 3D template, and the same spread spectrum techniques to generate the watermark. The use of Fourier transform ensures the same rotation, scaling, and proportion invariances. We have also a full invariant 3D watermark for theses blocks, exactly as for 2D still image watermarking. These 3D blocks may be rather large, or small enough to ensure more robustness against cropping. As for individual frame marking, we can use the same watermark for all blocks, or a different watermark for each block. The advantage of this spatio temporal approach is to take in account the motion and scene variation in watermarking, as developped in the paper of M.D. Swanson, B. Zhu and A.H. Tewfik, "Multiresolution Scene-Based Video Watermarking using Perceptual Models", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, May 1998. However, in contrast with our apparatus,

they make use of 1D temporal wavelets transform instead of our 3D Fourier transform.

IV. Properties of the watermark:

In the following, some of the properties of the watermark generated using the steps described above are discussed.

Resistance to cropping:

One feature of translation invariants developed using the Fourier transform is that they are invariant to circular translations (or cyclic shifts). This is used to construct watermarks that are invariant to cropping. This is illustrated by reference to Figs. 11 and 12.

As mentioned above, the image is split into blocks and the watermark is applied to each block. In other words, the same modulation pattern is applied to the Fourier components of each block, wherein the modulation pattern is given by the corresponding encoded messages **m**.

Fig. 11 shows such an image where the fat lines 100 designate the borders between the blocks. Suppose that the watermark in a standard size block will be of the form:

T=[A B ; C D]

where the sub-matrices A, B, C and D are of arbitrary size. A circular translation of such a watermark is of the form:

S=[D C ; B A].

The original stego-image is tiled with watermarks in the pattern [T T T T ; T T T T ; T T T T]. Therefore, a cropped section of the matrix will carry a watermark in the form [S S S S ; S S S S ; S S S S]. This is illustrated in Figure 12. When reading the watermark of

the cropped image of Fig. 12, each block carries the watermark S. Since S is a circular transform of T, it can be read without problems in the Fourier domain using the steps outlined above.

Note, however, that the cover image is not tiled, only the watermark is. Therefore, while cropping merely induces a circular translation of the watermark in each block, the change of image in each block is not a circular translation. To compensate for this, the phase components P_i of the Fourier transform must be used for correcting the sign of the modulation of the magnitude components M_i, as it is outlined under step 5 above.

The optimum size of block depends on a number of different factors. A size that is a power of two is useful because the FFT can be used. The block size also must be small enough to withstand cropping but large enough to comfortably contain a watermark. The best compromise for block size is 128.

Resistance to scaling and rotation:

As mentioned above, reading the RST template in log-polar space allows to detect and measure any scaling and/or rotation that was applied to the image. This information can then be used for reading the watermark. Since the reader knows the pattern that was used for modulating the magnitude components in step 5, he can identify the modulated components in the scaled and rotated image and derive the message **m'** therefrom. An alternative is to compensate the transformation using the measured rotation and scaling and read the message in the compensated image.

Note that the apparatus does not explicitly use a rotation and scale invariant watermark but instead searches the parameter space of rotations and scales. Since searching the space of rotation and scales in the frequency or space domain is quite complicated (as e.g. described in the WO 96/36163), the log-polar map is used

where these parameters are Cartesian coordinates and can be searched using efficient correlation techniques.

Resistance to change in aspect ratio:

Similarly as above, reading the PST template in log-log space allows to detect and measure the horizontal and vertical scaling that was applied to the image or video frame. This information can then be used to compensate the transformation, which the allows the watermark to be read.

The use of the log-polar map (LPM) or log-log map (LLM) changes depending on whether the watermark was inserted block by block of predefined size in the FFT domain or whether the block size depends on the image size. In the first case, the LPM or LLM is used to detect scale changes in the image. In the latter case, the maps are used to detect the ratio between the FFT size used in embedding (which is unknown since the original image size is unknown in oblivious watermarking) and the FFT size used in extraction, which equals the size of the image in which we attempt to extract the watermark. This is important in cases where the image size has changed as a result of e.g. cropping or rotation since the relative positions of the FFT points change.

Lossy compression:

The robustness of the watermark to operations such as lossy compression is achieved by using a perceptually adaptive spread spectrum communications approach, in which a spread spectrum signal is embedded in selected components of the magnitude spectrum of the Fourier Transform of the image.

Redundancy:

The watermark is embedded in blocks of a fixed size with exactly the same watermark embedded in each block. This means that the watermark can be recov-

ered from a single block only. This leads to a redundancy that increases the chance of extracting the watermark correctly from more than one block.

V. Summary

The following summarizes some of the properties of the preferred embodiments of the invention.

The use of an asymmetric cryptographic key pair for the seed generation enables the execution of asymmetric key agreement protocols with message recovery or appendix and the protection of the communication between the involved parties. Different security services for the communication, such as mutual authentication, integrity, confidentiality and non-repudiation are supported by the system with one asymmetric cryptographic key pair of the watermark author only for a registration or trading process

The present technique enables a strong binding relation between the image ID, the image, and the CH if the CH registers his copyright at the CCC. If an image is watermarked later by an unauthorized person, the time stamp in the copyright certificates resolves the copyright ownership.

The CH does not have to reveal his private cryptographic key if ownership verification has to be applied by a different legal party.

The present technique supports transferal of copyrights. If copyright is transferred to another legal party, corresponding copyright revocation certificates may be generated.

Digital signatures techniques are applied for the security of the communication between different parties and the authentication data embedded in a private or public watermark of an image or video. No signature labeling techniques of the complete image or video are applied by the system.

In addition, originality protection and image content protection by ciphering/deciphering in the transform domain is supported.

The Fourier Mellin transform is the Fourier Transform of a log-polar map. It allows to embed a watermark in a domain that is invariant to rotation, scale and translation. However this approach is costly and difficult to implement, and therefore it has been enhanced by combining with a Fourier Transform based template embedding technique.

In the present invention, the log-polar map of a Fourier transform is used as a means of facilitating rotation and scaling invariance. In order to be invariant to scaling and change of proportion, the log-log map of the Fourier transform is also used.

Circular translation invariants are used as a means of constructing digital watermarks that are invariant to cropping.

In contrast to some known techniques, the present system does not require a database of all watermarks that were ever embedded in image anywhere.

Information is embedded and/or retrieved in the log-polar or log-log domain of the Fourier transform. Frequency components are modulated which are oblivious to the cover image but which also have the property that they form an unambiguous non-repeated pattern in log-polar respectively log-log space. They are used for determining the degree of rotation and scaling respectively the change of proportion suffered by a stego-image in the absence of the cover-image. Coprime frequencies are useful for generating such a pattern or template. Uniform random sampling of log-polar or log-log space is another method that can be applied.

The technique applies a new concept of invariants which eliminate the need for explicitly searching for rotation and/or scaling values.

The methods described above can be incorporated into an apparatus, such as one or more computers, using know programming and hardware techniques. To prove the feasibility of the approach, a Java based copyright protection and authentication environment for digital images has been implemented. The PKI, the CH, the CCC, and the IB application processes all implement a Graphical User Interface and a server, supporting both console users and other requests through a socket interface.

While there are shown and described presently preferred embodiments of the invention, it is to be distinctly understood that the invention is not limited thereto but may be otherwise variously embodied and practiced within the scope of the following claims.

Claims

1. A method for generating and transmitting a data set between two parties H and B comprising the steps of

a) providing a cover data set (CD) corresponding to the data set to be transmitted,

b) generating a stego data set (SD) of said cover data set (CD) by embedding at least one digital watermark in said cover data set (CD), wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair (ps_H, vs_H) of H, said key pair comprising a secret private key (ps_H) and a known public key (vs_H) derived therefrom,

c) encrypting said stego data set (SD) using said key pair (ps_H, vs_H) of H,

d) transmitting said encrypted stego data set from said party H to said party B.

2. The method of claim 1, wherein said step c) comprises

generating a mask message (B||SN),

generating a signature ($DSSMR_G(ps_H, B||SN)$) of said mask message (B||SN) using said secret private key (ps_H), and

using said signature of said mask message for seeding an encryption algorithm for said stego data set (SD).

3. The method of claim 2 wherein said signature ($DSSMR_G(ps_H, B||SN)$) of said mask message (B||SN) is transmitted from H to B.

4. The method of one of the claims 2 or 3 wherein said encryption algorithm comprises the step of calculating the Fourier transform of said stego data set (SD), modifying the phase components of the Fourier

transform using a pseudo-random pattern seeded by said signature ($DSSMR_G(ps_H, B||SN)$) of said mask message ($B||SN$) and calculating the inverse Fourier transform for generating the encrypted stego data set.

5. The method of one of the preceding claims wherein said key pair (ps_H, vs_H) of H is an elliptic curve key pair.

6. The method of one of the preceding claims wherein said step b) further comprises the step of generating at least a first watermark, wherein said first watermark is encoded using said private key (ps_H) of H.

7. The method of claim 6 wherein said first watermark is encoded using a hash value ($crh(ps_H)$) of said private key (ps_H) and can be decoded by using said hash value ($crh(ps_H)$).

8. The method of claim 6 wherein said first watermark is encoded using a hash value ($crh(OAD_{CD})$) of a signature (OAD_{CD}) generated using said private key (ps_H).

9. The method of one of the preceding claims wherein said step b) further comprises the step of generating at least one second watermark, wherein said second watermark comprises a payload ($pc_H[AM]$) derived from the Fourier transform of said stego data (SD).

10. The method of one of the preceding claims wherein said step b) comprises the steps of:

i) providing a message ($s_1, s_2, \ldots, s_M$) to be transmitted in said at least one watermark, said message consisting of a plurality of symbols;

ii) providing a pseudo random generator seeded with a seed value derived from at least one key of said key pair (ps_H, vs_H) of H or a hash value thereof,

iii) encoding said message using values from said pseudo random generator

iv) using the said encoded message (**m**) for embedding said watermark.

11. The method of claim 10 wherein said step iii) comprises:

for each of said symbols (s_i), generating a pseudo random sequence of numbers (v_1, v_2, ...) by a said pseudo random generator,

using the value of each said symbols (s_i) for selecting a sub-sequence within said pseudo random sequence for forming a symbol vector ($\mathbf{r}_i$); and

adding said symbol vectors ($\mathbf{r}_i$) to generate said encoded message (**m**).

12. The method of claim 11 comprising the following steps for decoding said message:

extracting a read-out message (**m'**) from said watermark, said read-out message being a vector having the same length, if erased elements are replaced by zero, as said symbol vectors ($\mathbf{r}_i$),

generating all possible values of said symbol vectors ($\mathbf{r}_i$) using said pseudo random generator seeded with said seed, and

calculating the cross-correlation between said pseudo random sequences of numbers (v_1, v_2, ...) and said read-out message (**m'**) for retrieving said symbols (s_i).

13. The method of claim 10 wherein said step iii) comprises:

for each bit (b_j) of said symbol sequence (s_1, s_2, ..., s_M), deriving pseudo random vectors ($\mathbf{r}_j{}^*$)

having elements 1 or -1 from a said pseudo random generator, which pseudo random generator preferably generates m-sequences or Gold codes, and

depending on the value of said bit (b_j), multiplying said pseudo random vector ($\mathbf{r}_j{}^*$) with +1 or -1 to generate a modified pseudo random vector, and adding said modified pseudo random vectors to generate an encoded message ($\mathbf{m}$).

14. The method of claim 13 comprising the following steps for decoding said message:

extracting a read-out message ($\mathbf{m}'$) from said watermark,

deriving said pseudo random vectors ($\mathbf{r}_j{}^*$) from said pseudo random generator seeded with a said seed, and

calculating the cross correlation between each of said pseudo random vectors ($\mathbf{r}_j{}^*$) and said read-out message ($\mathbf{m}'$) for retrieving the corresponding bit (b_j) of the said symbol sequence ($s_1, s_2, \ldots, s_M$).

15. The method of one of the claims 10 - 14 wherein the position of components to be modulated by each value of the encoded message ($\mathbf{m}$) is given by a pseudo random generator seeded by a key known by both H and B.

16. The method of one of the preceding claims comprising the step of encoding a message for being embedded in said watermark by using symbol based Reed Solomon codes as error control codes.

17. The method of one of the preceding claims wherein said step b) further comprises the step of calculating a logarithm of said cover data set (CD) before embedding said watermark for embedding said watermark in a perceptually flat domain.

18. A method for generating a stego data set (SD) from a cover data set (CD) especially for step b) of one of the preceding claims, comprising the steps of:

generating at least one message (ID_{CD}),

digitally signing said message (ID_{CD}) using an asymmetric cryptographic key pair (p_H, v_H) and a signature generating algorithm (DSSMR) with message recovery for generating a digital signature (OAD_{CD}), and

generating said stego data set (SD) of said cover data set (CD) by generating at least one digital watermark, wherein said digital signature (OAD_{CD}) is used for deriving a seed for generating said watermark.

19. Method for generating and verifying a watermark in a cover data set (CD) representing a two-dimensional cover image, especially for step b) of one of the preceding claims, comprising the following steps for generating said watermark

A) calculating the Fourier transform of at least part of cover data set (CD) for generating Fourier components of said cover image, and

B) modulating at least part of said Fourier components using a template modulation pattern (T'),

C) using the inverse Fourier transform for generating a stego data set (SD),

said method further comprising the following steps for verifying said watermark in a possibly scaled and/or rotated version of said stego data set (SD),

D) calculating the Fourier transform of the possibly scaled and/or rotated version of said stego data set (SD) for generating Fourier components of said stego data set,

E) calculating a log-polar or log-log transform of said Fourier components of said stego data set (SD), and

F) calculating the cross correlation between a log-polar or log-log transform (T) of said modulation pattern (T′) and said log-polar or log-log transform of said Fourier components of said stego data set for evaluating a scaling and/or rotation factor.

20. The method of claim 19 wherein said step B) further comprises the steps of

calculating a log-polar or log-log transform of said components of said cover data set for generating log-polar components,

modulating said log polar components using a log-polar or log-log transform (T) of said modulation pattern (T′).

21. A method for verifying a watermark in a possibly rotated and/or scaled version of a two or three dimensional stego data set (SD), comprising the steps of:

A) calculating a Fourier transform of said stego data set (SD),

B) calculating a log-polar or a log-log transform of said Fourier transform of said stego data set,

C) calculating the correlation between said log-polar or log-log transform and a template (T), which template is the log-polar or log-log transformation of said watermark.

22. The method of claim 21, wherein said step B) comprises the step of calculating the log-polar transform of said Fourier transform of said stego data set and said step C) comprises a step of detecting a rotation and either a uniform scaling suffered by said stego data set or a ratio between block size used in embedding and extraction of said watermark.

23. The method of claim 21, wherein said step B) comprises the step of calculating the log-log transform of said Fourier transform of said stego data set and said step C) comprises a step of detecting either a change in aspect ratio suffered by said stego data set or a change of aspect ratio between block sizes used in embedding and extraction of said watermark.

24. The method of claim 21, wherein the presence of said watermark is verified by means of a Bayesian approach to detect the presence of said watermark given a said key without decoding said watermark.

25. The method of one of the claims 21 - 24, further comprising at least one of the following steps:

i) pre-filtering said cover data by applying a windowing algorithm thereto, preferably Blackman, Hanning or Welch windowing, and/or

ii) calculating the variance or distribution of the Fourier transform locally for filtering outliers and noise, and/or

iii) locating local peaks in said Fourier transform and carrying out said step B) for these local peaks only, preferably transforming only the coordinates of these local peaks, and preferably using the log-log or log-polar transform of said coordinates for calculating said correlation,

iv) excluding low frequency data from said Fourier transform before carrying out said step B), and/or,

v) detecting a scaling and/or rotation in said step C), using said scaling and/or rotation for either a) scaling and/or or rotating said Fourier transform, calculating a scaled and/or rotated log-log or log-polar transform therefrom and correlating said rotated log-log or log-polar transform with said template, or b) calculating a second template by scaling and/or rotating

an original Fourier-space template and calculating a log-log and or log-polar transform therefrom and using said second template for calculation a second correlation with said log-log or log-polar transform of said stego data, and/or

vi) weighing low frequency components of said log-log or log-polar transform stronger that high frequency components while carrying out said correlation.

26. A method for generating a stego data set (SD) from a cover data set (CD) especially for step b) of one of the claims 1 - 18, comprising the step of modulating said cover data set (CD) using a given pattern, which pattern is calculated from a watermark using the following steps:

A) providing said watermark,

B) calculating a first inverse Fourier transform of said watermark,

C) calculating an inverse log-log or log-polar transform of said watermark, and

D) calculating said pattern from said inverse log-log or log-polar transform.

27. The method of claim 26 further comprising the step of combining the magnitude components of said first inverse Fourier transform with the phases of a Fourier transform of said stego data (SD) to generate a frequency space pattern and, preferably, calculating a second inverse Fourier transform of said frequency space pattern.

28. A method for verifying a watermark in a possibly rotated and/or scaled version of a two or three dimensional stego data set (SD), preferably as generated in one of the claims 25 or 26, comprising the steps of:

A) calculating a first Fourier transform of said stego data set (SD),

B) calculating a log-polar or a log-log transform of said Fourier transform of said stego data set,

C) calculating a second Fourier transform of said log-polar or log-log transform and searching said watermark in said second Fourier transform.

29. A method for generating a watermark in a cover data set (CD) representing a two or three dimensional data set, especially for step b) of one of the preceding claims, comprising the following steps:

A) generating a template modulation pattern (T′) using a random number generator seeded by a key (K),

B) calculating the Fourier transform of at least part of said cover data set (CD) for generating Fourier components of said cover data set,

C) modulating at least part of said Fourier components using said template modulation pattern (T′),

D) using the inverse Fourier transform for generating a stego-image.

30. Method for generating a watermark in a cover data set (CD) representing a cover image especially for one of the preceding claims, characterized by the step of dividing said image into a plurality of blocks and by the following steps carried out for each block:

i) calculating the Fourier transform of the block,

ii) modulating at least part of the magnitude components of the Fourier transform of the block using a modulation pattern, which modulation pattern defines values to be added/subtracted to/from said magnitude components, wherein for each magnitude component its corresponding phase component determines if said value is to be added or subtracted, and wherein the same modulation pattern is used for all blocks.

31. The method of claim 30 wherein said blocks are adjacent.

32. The method of claim 30 wherein the said image is divided into a plurality of overlapping blocks and wherein the step i) comprises calculating the Lapped Orthogonal transform of each block to embed a Lapped Orthogonal transform based watermark.

33. The method of claim 30 wherein the said image is divided into a plurality of non-square blocks and wherein the step i) consists in padding each block with appropriate values (constant or symmetric extension) in order to obtain square blocks, calculating the Fourier transform of each obtained square block to embed Fourier transform based watermark.

34. The method of claim 30 wherein the said image is divided into a plurality of non-square blocks and wherein said step i) comprises computing the arbitrary length wavelet transform of each block to embed a wavelet transform based watermark.

35. The method of one of the claims 30 - 34 wherein the watermark is applied to all or some of the frames of a video.

36. A method for generating a stego data set (SD) from a cover data set (CD) especially for step b) of one of the claims 1 - 18, by adding a watermark to said cover data set, wherein said cover data set comprises video data, comprising the steps of

generating three dimensional spatio-temporal blocks of said video data and

applying said watermark to each of said blocks, preferably by calculating a Fourier transform of each of said blocks.

37. A method for generating a stego data set (SD) from a cover data set (CD) especially according to one of the preceding claims, by adding a watermark to said cover data set comprising the steps of

dividing said stego data sets into blocks,

calculating a lapped orthogonal transform (LOT) of each of said blocks, and

applying said watermark to said lapped orthogonal transforms.

38. The method of claim 37 further comprising the step of modulating selected components of said lapped orthogonal transform (LOT) as a function of a local image characteristics, such as the local image variance.

39. Method for generating and transmitting a data set between two parties H and B, especially of one of the preceding claims, comprising the steps of

providing a cover data set (CD) corresponding to the data set to be transmitted,

generating a stego data set (SD) of said cover data set (CI) at a party H by generating at least one digital watermark in said cover data set (CD),

transmitting a hash value of said stego data set (SD) to a registration party (O), and

permanently storing certification data (CCD) at said registration party (O), said certification data comprising said hash value of said stego data set (SI), a digital time stamp (TVP) and information designating said party H.

40. The method of claim 39 further comprising the steps of generating a digital signature of said certification data (CCD) using an asymmetric cryptographic key pair (ps_O, vs_O) of said registration party (O), transmitting said certification data (CCD) and said digi-

tal signature to said party H, and verifying said digital signature at said party H by using a public key (vs_O) of said key pair of said registration party.

41. A method for embedding a watermark in a cover data set for generating a stego data set, especially of one of the preceding claims, comprising the steps of

calculating at least some magnitude Fourier components (MC) of said cover data set (CD),

applying an authentication function (AF) for generating a value (AM) derived from said Fourier components (MC),

ciphering said value (AM) using a secret key (pc_H) of an asymmetric key pair (pc_H, vc_H) for generating a ciphered message, and

embedding said ciphered message as a payload in a public watermark.

42. A method for verifying the originality of a possibly modified stego data set generated with the method of claim 41 comprising the step of reading said value (AM) by decoding said ciphered message using the public key of said key par and comparing said magnitude Fourier components to said stego data set.

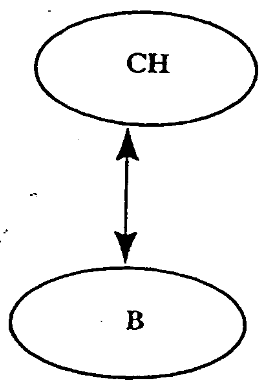


Fig. 1

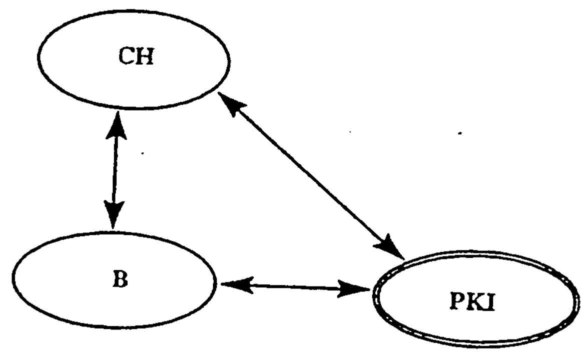


Fig. 2

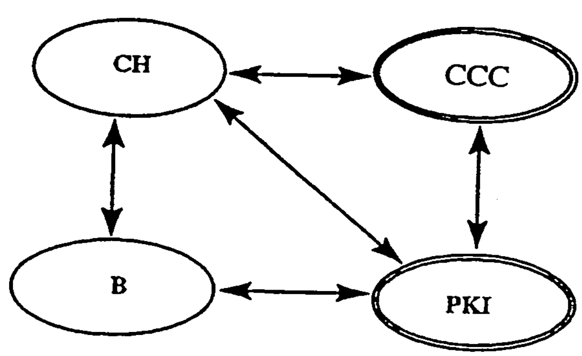


Fig. 3

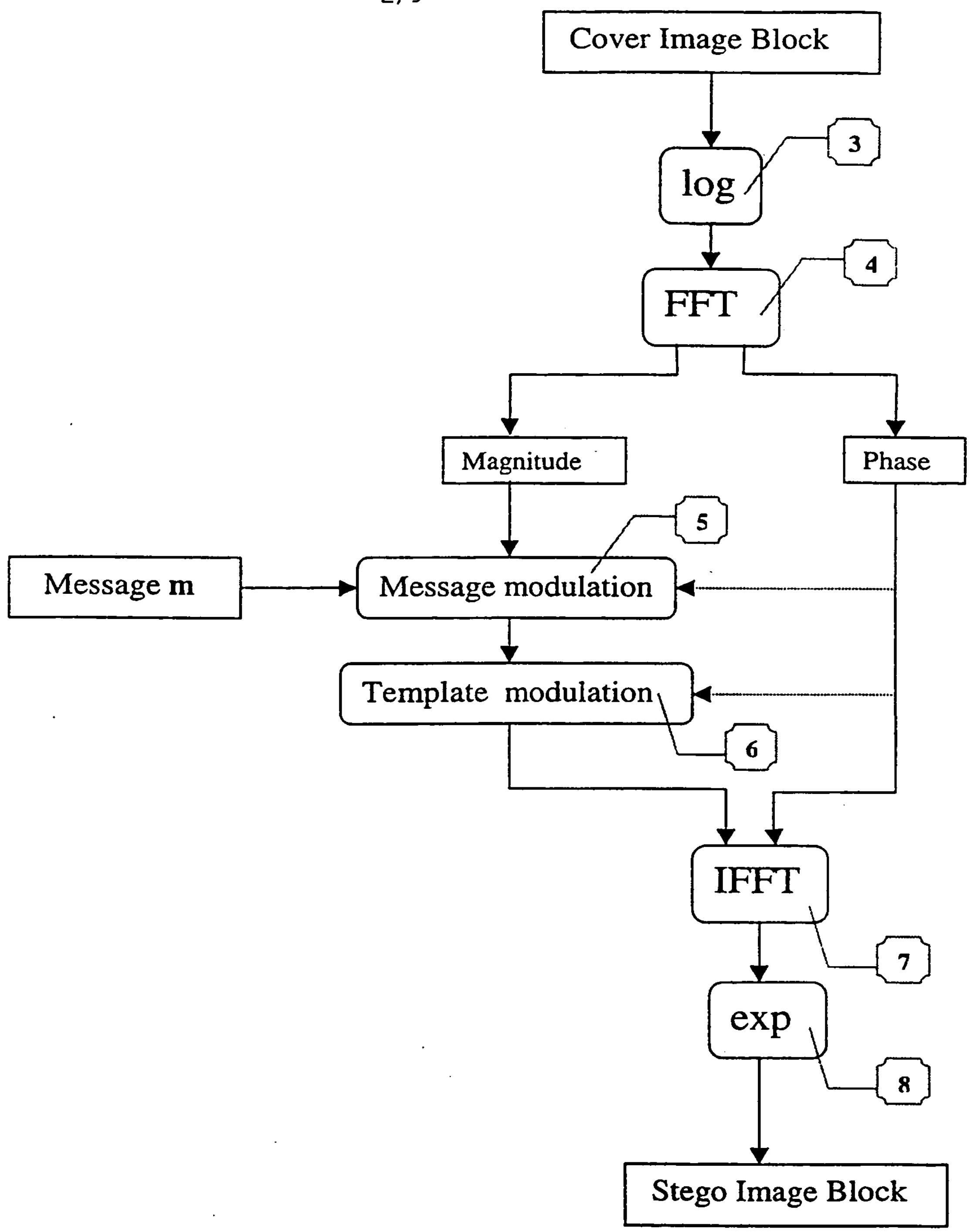

Cover Image Block
log
3
FFT
4
Magnitude
Phase
5
Message m
Message modulation
Template modulation
6
IFFT
7
exp
8
Stego Image Block

Fig 4.

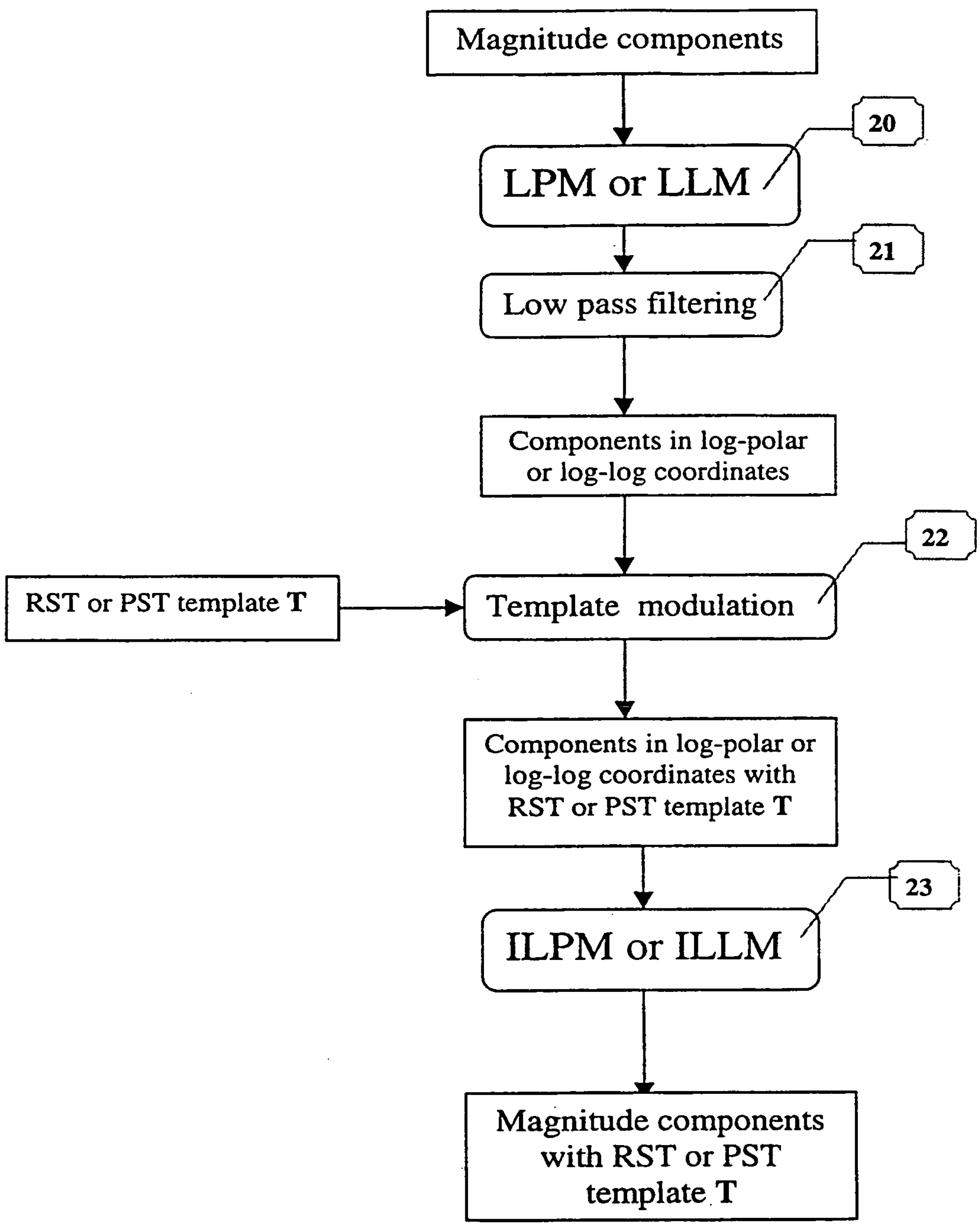

Magnitude components
LPM or LLM
20
Low pass filtering
21
Components in log-polar or log-log coordinates
RST or PST template T
Template modulation
22
Components in log-polar or log-log coordinates with RST or PST template T
ILPM or ILLM
23
Magnitude components with RST or PST template T

Fig 5.

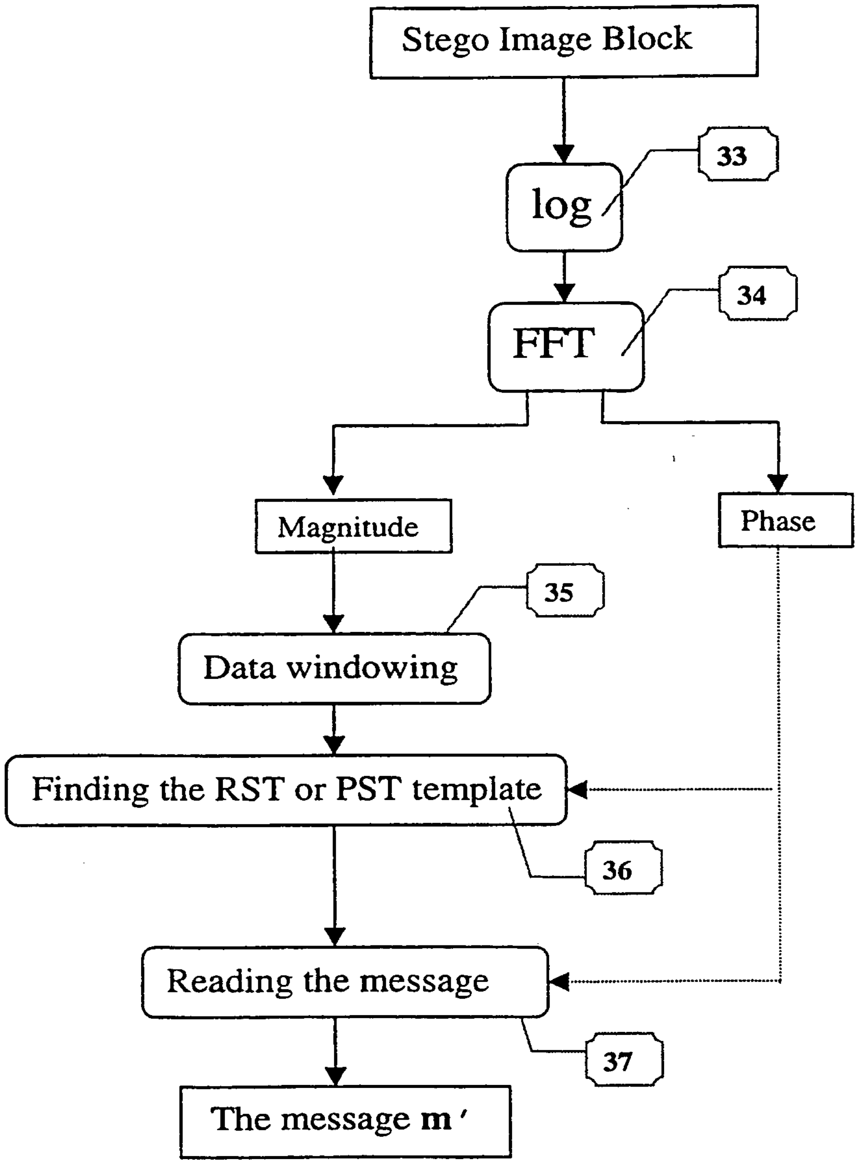

Stego Image Block
log
33
FFT
34
Magnitude
Phase
35
Data windowing
Finding the RST or PST template
36
Reading the message
37
The message m'

Fig 6.

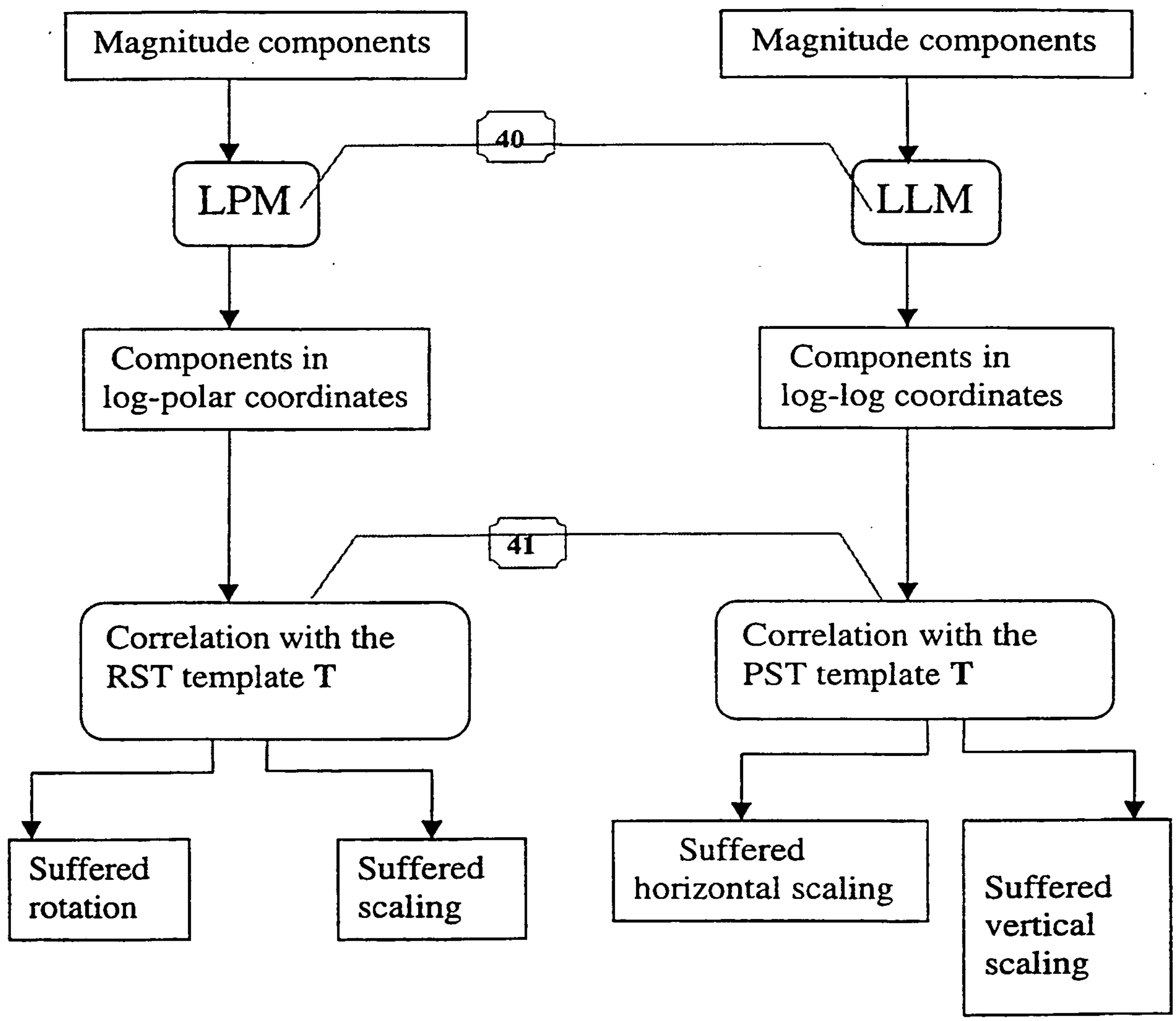

Magnitude components
Magnitude components
40
LPM
LLM
Components in log-polar coordinates
Components in log-log coordinates
41
Correlation with the RST template T
Correlation with the PST template T
Suffered rotation
Suffered scaling
Suffered horizontal scaling
Suffered vertical scaling

Fig 7.

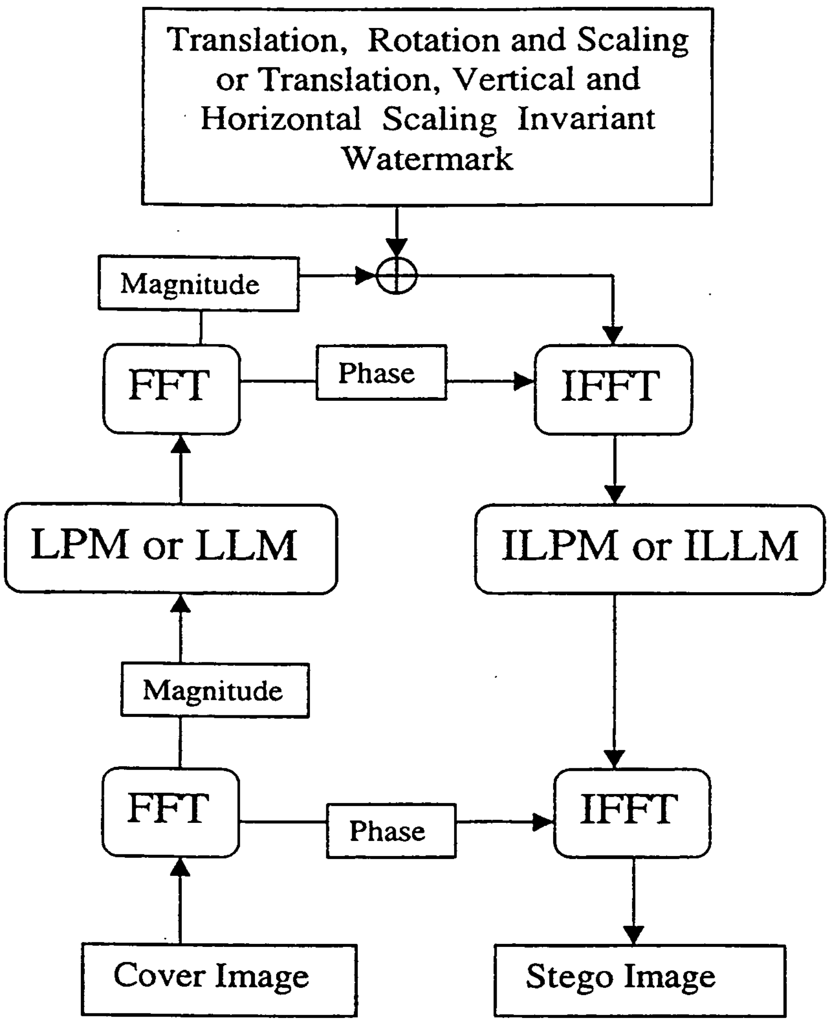

Translation, Rotation and Scaling or Translation, Vertical and Horizontal Scaling Invariant Watermark
Magnitude
FFT
Phase
IFFT
LPM or LLM
ILPM or ILLM
Magnitude
FFT
Phase
IFFT
Cover Image
Stego Image

Fig 8.

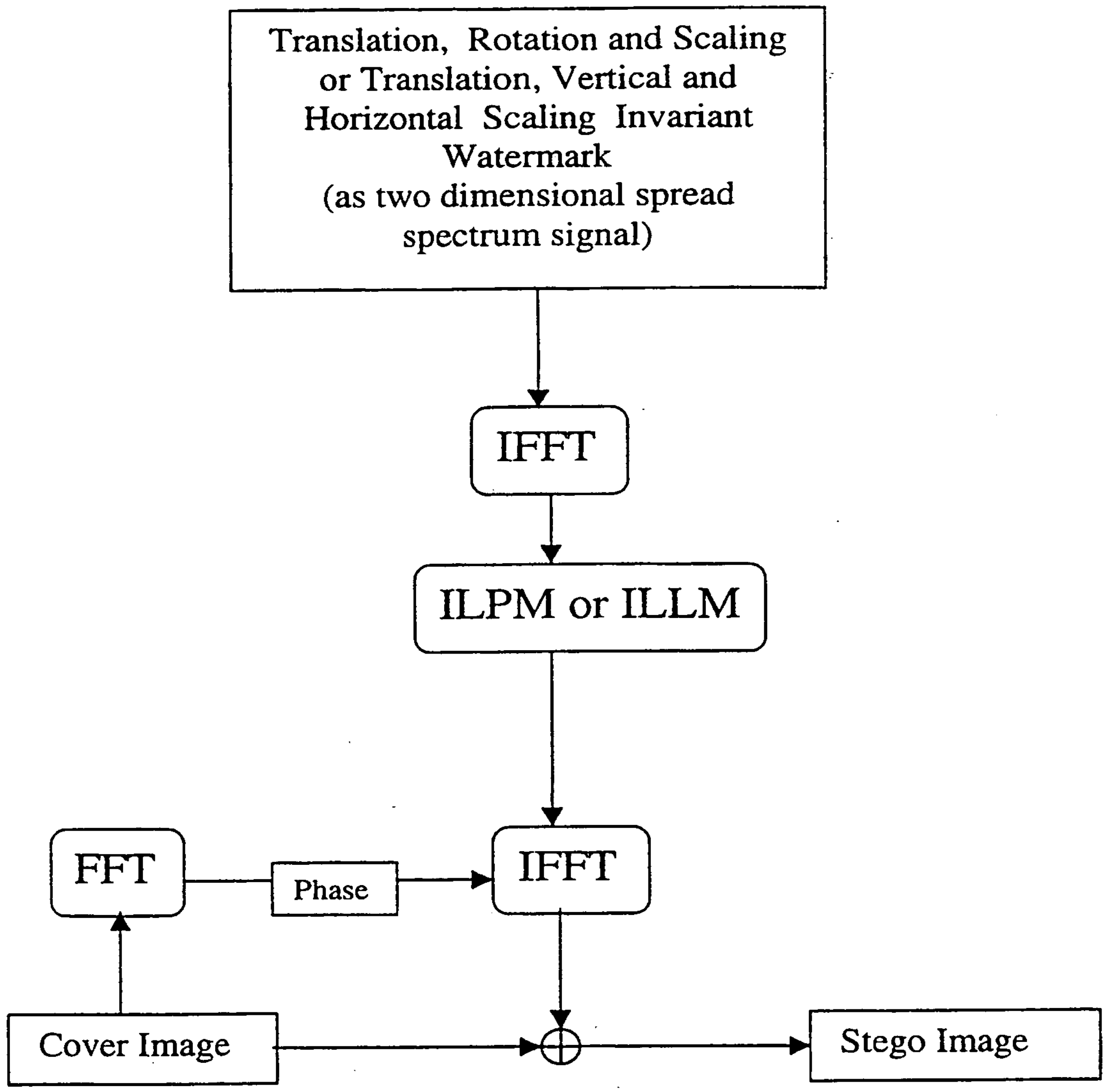

Translation, Rotation and Scaling or Translation, Vertical and Horizontal Scaling Invariant Watermark (as two dimensional spread spectrum signal)
IFFT
ILPM or ILLM
FFT
Phase
IFFT
Cover Image
Stego Image

Fig 9.

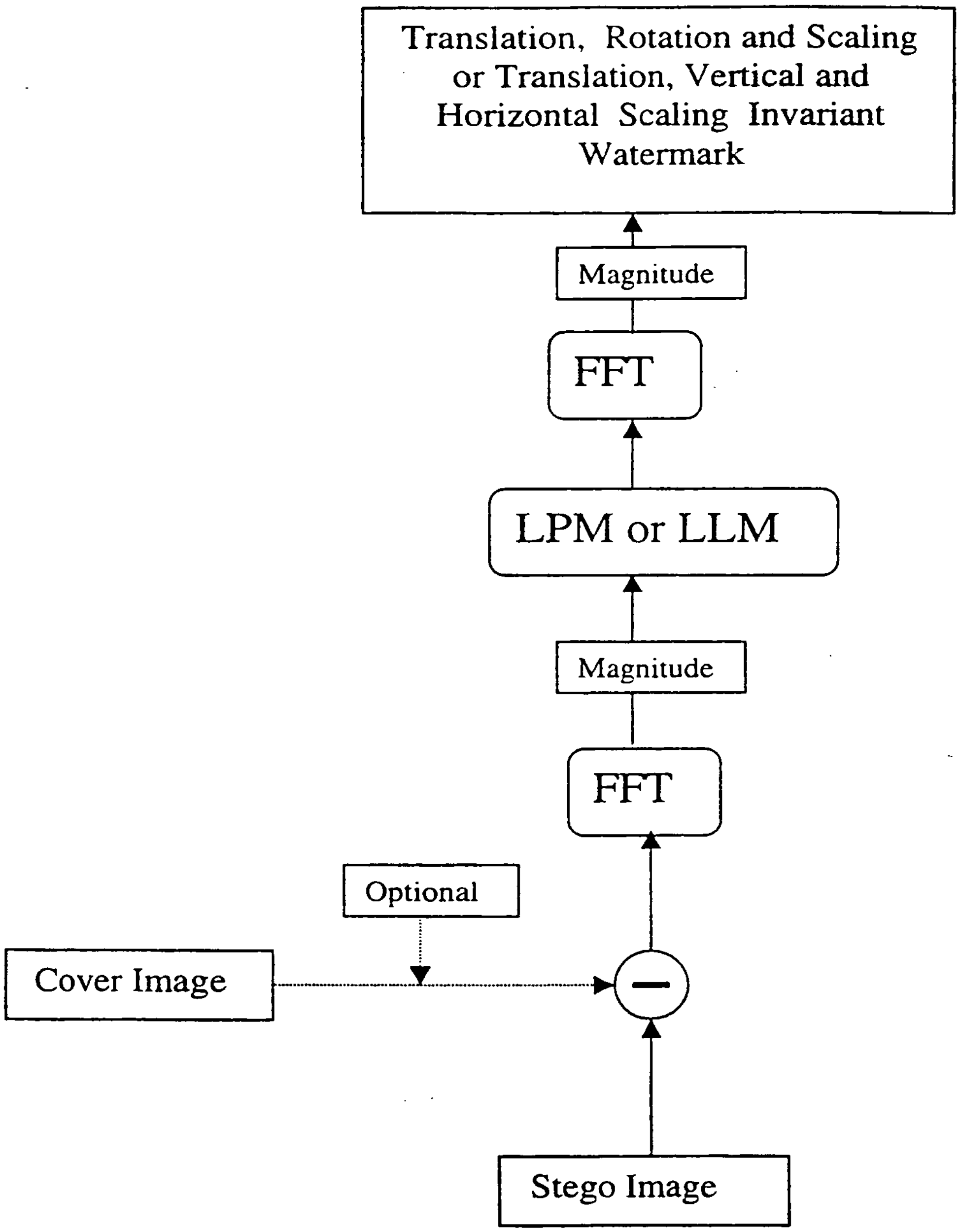

Translation, Rotation and Scaling or Translation, Vertical and Horizontal Scaling Invariant Watermark
Magnitude
FFT
LPM or LLM
Magnitude
FFT
Optional
Cover Image
Stego Image

Fig 10.

100

A	B	A	B	A	B	A	B
C	D	C	D	C	D	C	D
A	B	A	B	A	B	A	B
C	D	C	D	C	D	C	D
A	B	A	B	A	B	A	B
C	D	C	D	C	D	C	D

Fig. 11

D	C	D	C	D	C
B	A	B	A	B	A
D	C	D	C	D	C
B	A	B	A	B	A

Fig. 12

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 98/01500

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N1/32 H04N7/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996, pages 99-110, XP000604065 cited in the application	1
A	see the whole document	2,5-9,18

Y	EP 0 534 419 A (IBM) 31 March 1993 cited in the application	1
A	see page 8, line 36 - page 9, line 20	2,5-9,18

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 December 1998	08/12/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hazel, J

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KIYOSHI TANAKA ET AL: "A DIGITAL SIGNATURE SCHEME ON A DOCUMENT FOR MH FACSIMILE TRANSMISSION" ELECTRONICS & COMMUNICATIONS IN JAPAN, PART I - COMMUNICATIONS, vol. 74, no. 8, 1 August 1991, pages 30-36, XP000287493 cited in the application see Sections 1 and 2	1,2,18
A	ZHAO J ET AL: "EMBEDDING ROBUST LABELS INTO IMAGES FOR COPYRIGHT PROTECTION" PROCEEDINGS OF THE KNOWRIGHT. CONFERENCE. PROCEEDINGS OF THE INTERNATIONAL CONGRESS ON INTELECTUAL PROPERTY RIGHTS FOR SPECIALIZED INFORMATION, KNOWLEGDE AND NEW TECHNOLOGY,21 August 1995, pages 242-251, XP000603945 cited in the application see Section 2	1
X	FR 2 740 897 A (AETA APPLIC ELECTRONIQUES TECH) 9 May 1997	36
A	see page 3, line 31 - page 5, line 19; claim 1	4,19,21, 28,30, 31,35, 37,41
A	WO 96 36163 A (RHOADS GEOFFREY B ;DIGIMARC CORP (US)) 14 November 1996 see page 80, line 7 - page 84, line 9	4,19,28, 29
A	WO 96 27259 A (HIGHWATER FBI LIMITED ;HILTON DAVID (GB)) 6 September 1996 see page 16, line 33 - page 17, line 14	4,19,28, 29
A	RUANAIDH J J K O ET AL: "PHASE WATERMARKING OF DIGITAL IMAGES" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING (IC, LAUSANNE, SEPT. 16 - 19, 1996, vol. 3, 16 September 1996, pages 239-242, XP000199952 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS see the whole document	4,29-31
A	EP 0 766 468 A (NIPPON ELECTRIC CO) 2 April 1997 see column 11, line 4 - column 12, line 2	4,29-31
A	EP 0 777 197 A (EASTMAN KODAK CO) 4 June 1997 see page 4, line 36 - page 5, line 5	26

-/--

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 98/01500

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0534419 A	31-03-1993	US 5200999 A	06-04-1993
		CA 2075329 A,C	28-03-1993
		JP 5216409 A	27-08-1993
		JP 8016826 B	21-02-1996
FR 2740897 A	09-05-1997	NONE	
WO 9636163 A	14-11-1996	US 5832119 A	03-11-1998
		US 5822436 A	13-10-1998
		US 5748783 A	05-05-1998
		AU 6022396 A	29-11-1996
		CA 2218957 A	14-11-1996
		EP 0824821 A	25-02-1998
WO 9627259 A	06-09-1996	AU 4885296 A	18-09-1996
		EP 0813788 A	29-12-1997
EP 0766468 A	02-04-1997	AU 6584096 A	10-04-1997
		CA 2184949 A	29-03-1997
		JP 9191394 A	22-07-1997
EP 0777197 A	04-06-1997	JP 9191395 A	22-07-1997
EP 0539726 A	05-05-1993	US 5164988 A	17-11-1992
		CA 2071413 A	01-05-1993
		JP 2552061 B	06-11-1996
		JP 5216411 A	27-08-1993

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

1. Claims: 1-18,41,42
Method for embedding a digital watermark in a data set or digitally signing a message using at least one of an asymmetric cryptographic key pair

2. Claims: 19-38
Method for generating a digital watermark in a data set and/or for verifying a watermark, comprising calculating a transform

3. Claims: 39-40
Method for generating a digital watermark in a data set, for transmitting a hash value of a stego data set to a registration party and for storing certification data there

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 98/01500

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No
PCT/IB 98/01500

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 539 726 A (IBM) 5 May 1993	
A	ZHAO ET AL: "A www service to embed and prove digital copyright watermarks" PROCEEDINGS OF THE EUROPEAN CONFERENCE ON MULTIMEDIA APPLICATIONS, SERVICES AND TECHNIQUES, vol. 2, 28 - 30 May 1996, pages 695-709, XP000199921 Louvain la Neuve (BE) see Section 4	39,40
A	DELAIGLE J.-F. ET AL: "DIGITAL IMAGES PROTECTION TECHNIQUES IN A BROADCAST FRAMEWORK: AN OVERVIEW" PROCEEDINGS OF THE EUROPEAN CONFERENCE ON MULTIMEDIA APPLICATIONS, SERVICES AND TECHNIQUES, vol. 2, 28 - 30 May 1996, pages 711-727, XP000199920 Louvain la Neuve (BE) see Section 4	39,40

2